

Instalación servidor DNS

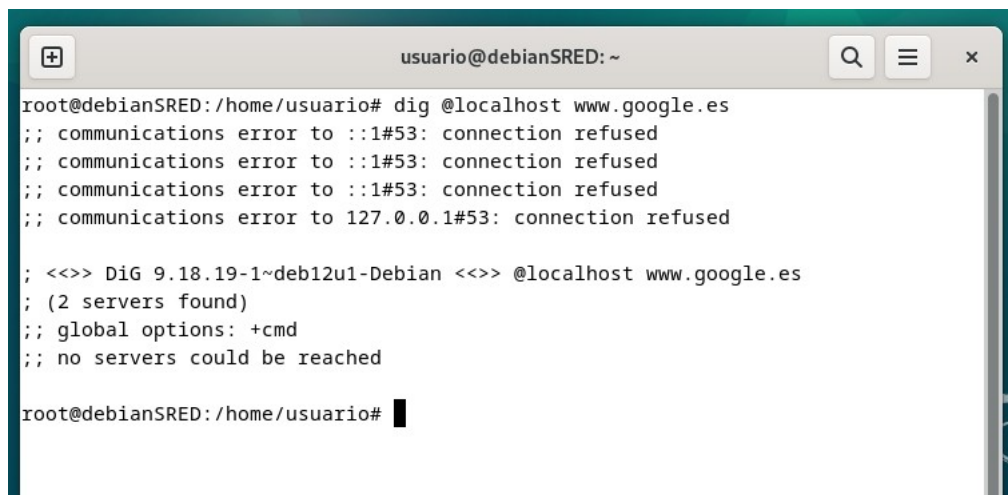
Índice

1. Instalación BIND versión 9.....	3
1.2 Sobre el BIND 9.....	5
2. Configuración DNS maestro.....	8
2.1 Configuración.....	10
2.2 Comprobación.....	14
3. Configuración DNS Esclavo.....	15
3.1 Configuración.....	17
3.2 Comprobación.....	20

1. Instalación BIND versión 9

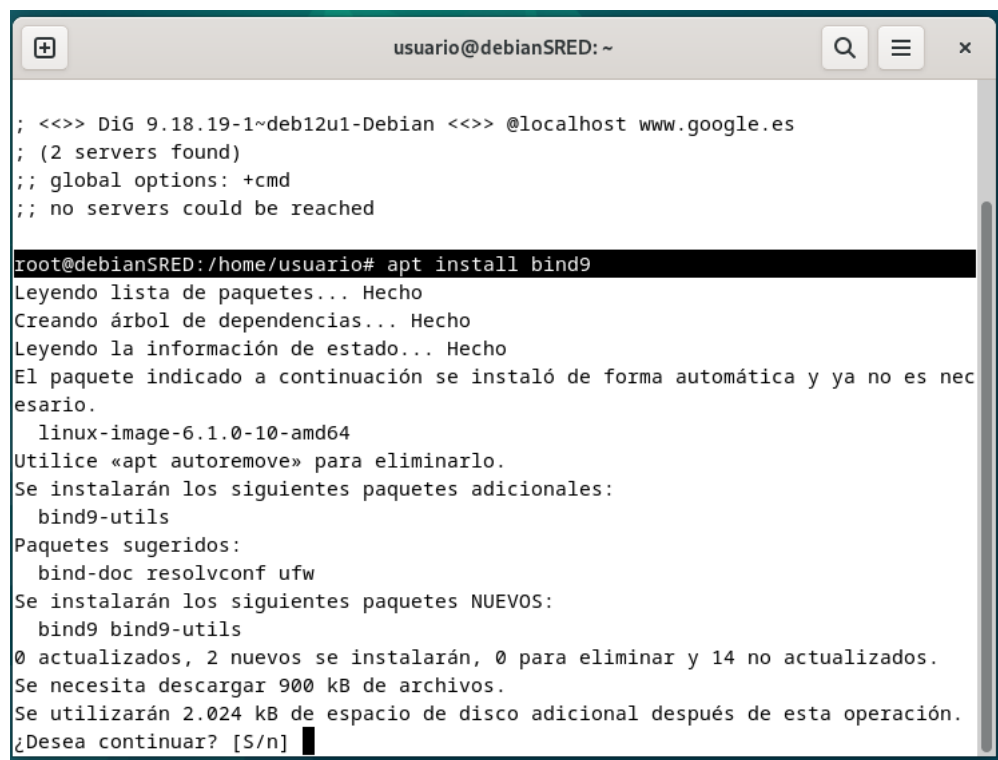
Bind 9 es un tipo de servidor DNS. El mas utilizado en internet, sobre todo en sistemas Unix. Lo instalaremos en una MV para que se convierta en dicho servidor DNS.

Antes de su instalación comprobamos que nuestra MV no es un dominio o servidor DNS. Vemos que no existe comunicación.



```
usuario@debianSRED: ~  
root@debianSRED:/home/usuario# dig @localhost www.google.es  
;; communications error to ::1#53: connection refused  
;; communications error to ::1#53: connection refused  
;; communications error to ::1#53: connection refused  
;; communications error to 127.0.0.1#53: connection refused  
  
; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @localhost www.google.es  
; (2 servers found)  
;; global options: +cmd  
;; no servers could be reached  
  
root@debianSRED:/home/usuario#
```

Ahora si, instalamos BIND 9 y hacemos la misma comprobación.



```
usuario@debianSRED: ~  
; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @localhost www.google.es  
; (2 servers found)  
;; global options: +cmd  
;; no servers could be reached  
  
root@debianSRED:/home/usuario# apt install bind9  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.  
  linux-image-6.1.0-10-amd64  
Utilice «apt autoremove» para eliminarlo.  
Se instalarán los siguientes paquetes adicionales:  
  bind9-utils  
Paquetes sugeridos:  
  bind-doc resolvconf ufw  
Se instalarán los siguientes paquetes NUEVOS:  
  bind9 bind9-utils  
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 14 no actualizados.  
Se necesita descargar 900 kB de archivos.  
Se utilizarán 2.024 kB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n]
```

```

usuario@debianSRED: ~
root@debianSRED:/home/usuario# systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enable>
   Active: active (running) since Sat 2023-10-28 13:19:18 CEST; 41s ago
     Docs: man:named(8)
    Main PID: 3748 (named)
      Status: "running"
        Tasks: 4 (limit: 4709)
       Memory: 18.2M
          CPU: 29ms
    CGroup: /system.slice/named.service
            └─3748 /usr/sbin/named -f -u bind

oct 28 13:19:18 debianSRED named[3748]: network unreachable resolving './DNSKEY>
oct 28 13:19:18 debianSRED named[3748]: network unreachable resolving './NS/IN'>
oct 28 13:19:18 debianSRED named[3748]: network unreachable resolving './DNSKEY>
oct 28 13:19:18 debianSRED named[3748]: network unreachable resolving './NS/IN'>
oct 28 13:19:18 debianSRED named[3748]: network unreachable resolving './DNSKEY>
oct 28 13:19:18 debianSRED named[3748]: network unreachable resolving './NS/IN'>
oct 28 13:19:18 debianSRED named[3748]: network unreachable resolving './DNSKEY>
oct 28 13:19:18 debianSRED named[3748]: network unreachable resolving './NS/IN'>
oct 28 13:19:19 debianSRED named[3748]: managed-keys-zone: Initializing automat>
oct 28 13:19:19 debianSRED named[3748]: resolver priming query complete: success
lines 1-22/22 (END)

```

Lo reiniciamos. Comprobamos con el dig, y vemos que existe comunicación.

```

usuario@debianSRED: ~
root@debianSRED:/home/usuario# systemctl restart bind9
root@debianSRED:/home/usuario# dig @localhost www.google.es

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @localhost www.google.es
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 25710
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: c1eefd0a0969c9d601000000653ceeb18c2e30232a98adb4 (good)
;; QUESTION SECTION:
;www.google.es.                IN      A

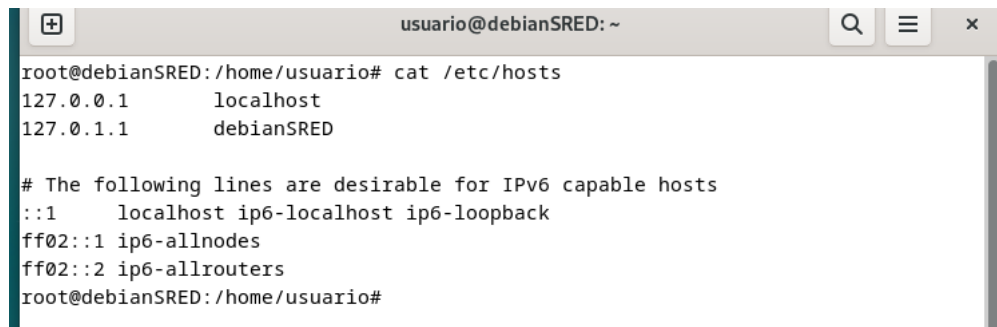
;; Query time: 128 msec
;; SERVER: ::1#53(localhost) (UDP)
;; WHEN: Sat Oct 28 13:21:21 CEST 2023
;; MSG SIZE rcvd: 70

root@debianSRED:/home/usuario#

```

1.2 Sobre el BIND 9.

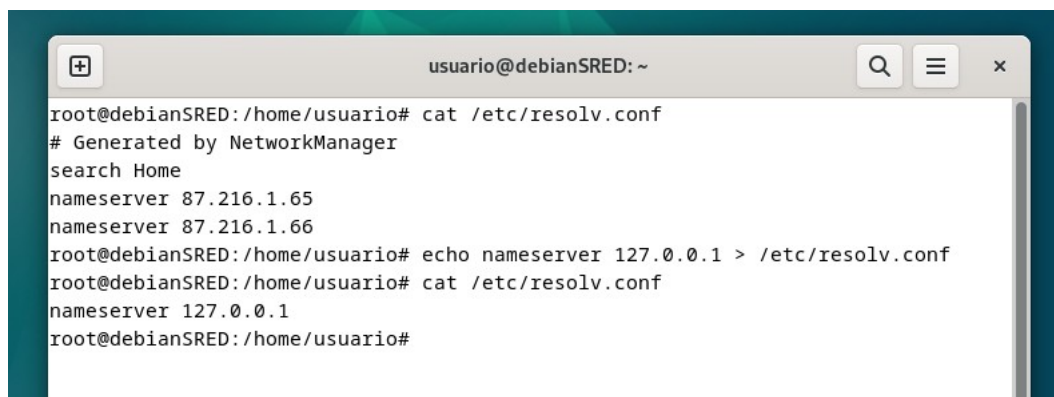
El comando `dig` permite especificar el servidor que queremos que haga la traducción, para ello se usa el símbolo `@` junto con el nombre o dirección del servidor DNS; en el ejemplo se ha puesto `@localhost`, donde `localhost` se ha traducido vía el fichero `/etc/hosts` en el que aparece con la dirección `127.0.0.1` (`::1 IPv6`), es decir, el equipo local, donde acabamos de instalar BIND.

A terminal window titled 'usuario@debianSRED: ~' showing the command 'cat /etc/hosts' being executed. The output lists IP addresses and their corresponding hostnames: 127.0.0.1 localhost, 127.0.1.1 debianSRED, and IPv6 addresses for localhost, allnodes, and allrouters.

```
root@debianSRED:/home/usuario# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      debianSRED

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

Sabiendo esto, ya podemos cambiar el fichero `/etc/resolv.conf` para que se use siempre nuestro servidor BIND (Al reiniciar el equipo se cambia, por lo que cada vez que encendamos la MV tenemos que volver a repetirlo).

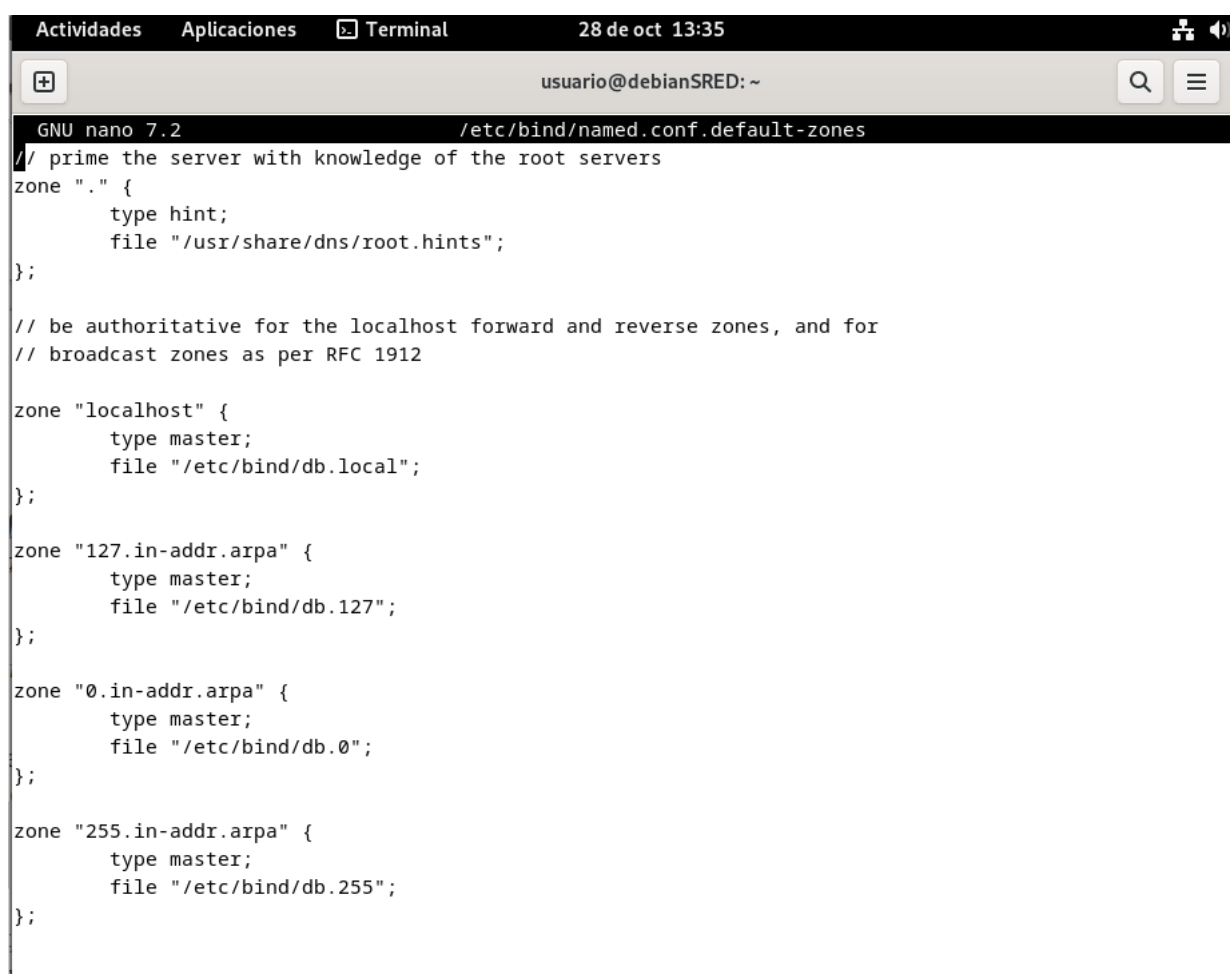
A terminal window titled 'usuario@debianSRED: ~' showing the process of updating /etc/resolv.conf. It first displays the current content, then shows the command to replace it with 'nameserver 127.0.0.1', and finally shows the updated content.

```
root@debianSRED:/home/usuario# cat /etc/resolv.conf
# Generated by NetworkManager
search Home
nameserver 87.216.1.65
nameserver 87.216.1.66
root@debianSRED:/home/usuario# echo nameserver 127.0.0.1 > /etc/resolv.conf
root@debianSRED:/home/usuario# cat /etc/resolv.conf
nameserver 127.0.0.1
root@debianSRED:/home/usuario#
```

La configuración de BIND se encuentra en ***named.conf***, la cual se distribuye, con la instrucción ***include***, entre los ficheros: ***named.conf.options***, ***named.conf.local*** y ***named.conf.default-zones***.

- ***named.conf.options***: En este fichero se encuentra la instrucción ***options*** que es donde se incluyen todos los parámetros a nivel global de BIND.
- ***named.conf.local***: Aquí es donde crearemos nuestras zonas con la instrucción ***zone***.
- ***named.conf.default-zones***: Este fichero contiene las instrucciones zone de algunas zonas que incluye BIND por defecto.

En nuestro caso, nos centraremos en el fichero ***..default-zones***, ya que es donde se encuentran las zonas, y es donde estableceremos nuestro propio dominio mas adelante (Ahora el nombre del dominio es ***localhost***, el tipo de zona es ***master***, por lo que el servidor es autoritario sobre la zona, y ***file*** señala al fichero de zona donde están los RR). Vemos el fichero.



```
GNU nano 7.2 /etc/bind/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.local";
};

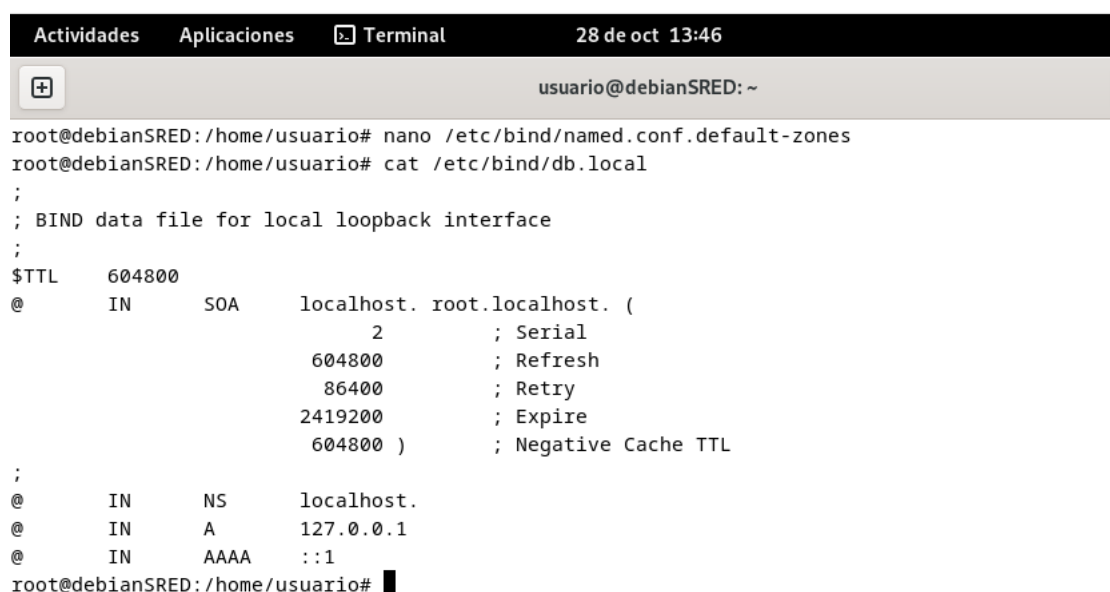
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

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

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

La primera “zone” que vemos es la zona raíz, y las siguientes, son zonas por defecto instaladas con el bind 9.

Como vemos son todos ficheros db., ficheros de zona, que BIND carga por defecto, pues se han creado en *named.conf.default-zones*. Pero nos centraremos en el db.local, ya que permitirá resolver el nombre *localhost* a *127.0.0.1*. Ahora mismo, dicho nombre se resuelve vía */etc/hosts*, pero si se elimina, se puede seguir utilizando, pues BIND lo traduce, sin que nosotros hagamos nada, gracias a *db.local*.



```

Actividades  Aplicaciones  Terminal  28 de oct 13:46
+-----+
+ | usuario@debianSRED: ~ | +-----+
+-----+
root@debianSRED:/home/usuario# nano /etc/bind/named.conf.default-zones
root@debianSRED:/home/usuario# cat /etc/bind/db.local
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      localhost. root.localhost. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      A        127.0.0.1
@         IN      AAAA     ::1
root@debianSRED:/home/usuario#

```

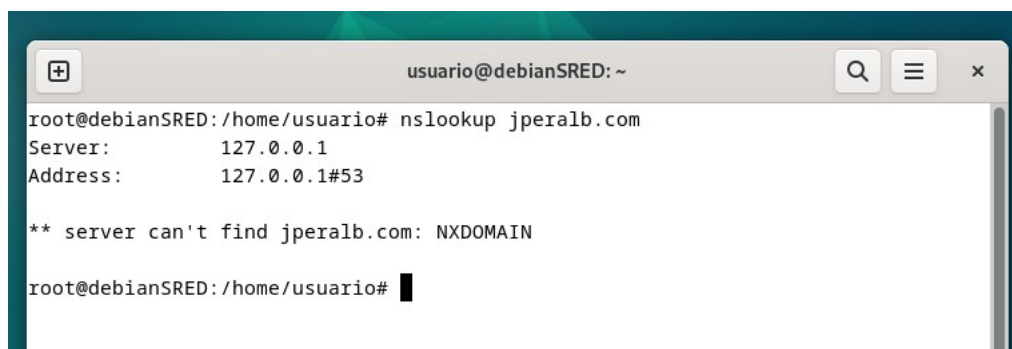
Como se ve en el fichero de zona, solo se asocia un RR A al nombre del dominio (@ IN A 127.0.0.1), por lo que el nombre *localhost* se traduce a 127.0.0.1 (::1 en caso de IPv6). Estrictamente esta zona sirve para traducir nombres como *www.localhost*, pero únicamente está pensada para traducir el nombre *localhost*, por eso solo hay un RR A para el dominio, y no para otros nombres

Una vez sabemos esto, ya podemos configurar el servidor maestro.

2. Configuración DNS maestro.

En primer lugar, hay que señalar que estableceremos una zona master para este apartado. Esta zona, proporciona, datos autoritarios de la zona o dominio (servidor que contiene los registros de recursos para una zona (SOA y NS), el fichero de zona se aloja en el disco local del servidor, y el servidor de la zona *master* responderá a las solicitudes de transferencia de zona de los servidores de zonas *slave* (Cada zona puede tener uno o más servidores de nombres de dominio autoritarios. Uno de ellos debe ser primario. Si tiene varios, el resto pueden ser secundarios o caché).

Vamos a configurar un servidor maestro para el dominio *jperalb.com*. Vamos a comprobar si ya existe. Y no existe.

A terminal window titled 'usuario@debianSRED: ~' with search, menu, and close icons. The terminal shows a command 'nslookup jperalb.com' being executed. The output is: 'Server: 127.0.0.1', 'Address: 127.0.0.1#53', and '** server can't find jperalb.com: NXDOMAIN'. The prompt returns to 'root@debianSRED: /home/usuario#'.

```
usuario@debianSRED: ~
root@debianSRED:/home/usuario# nslookup jperalb.com
Server:      127.0.0.1
Address:     127.0.0.1#53

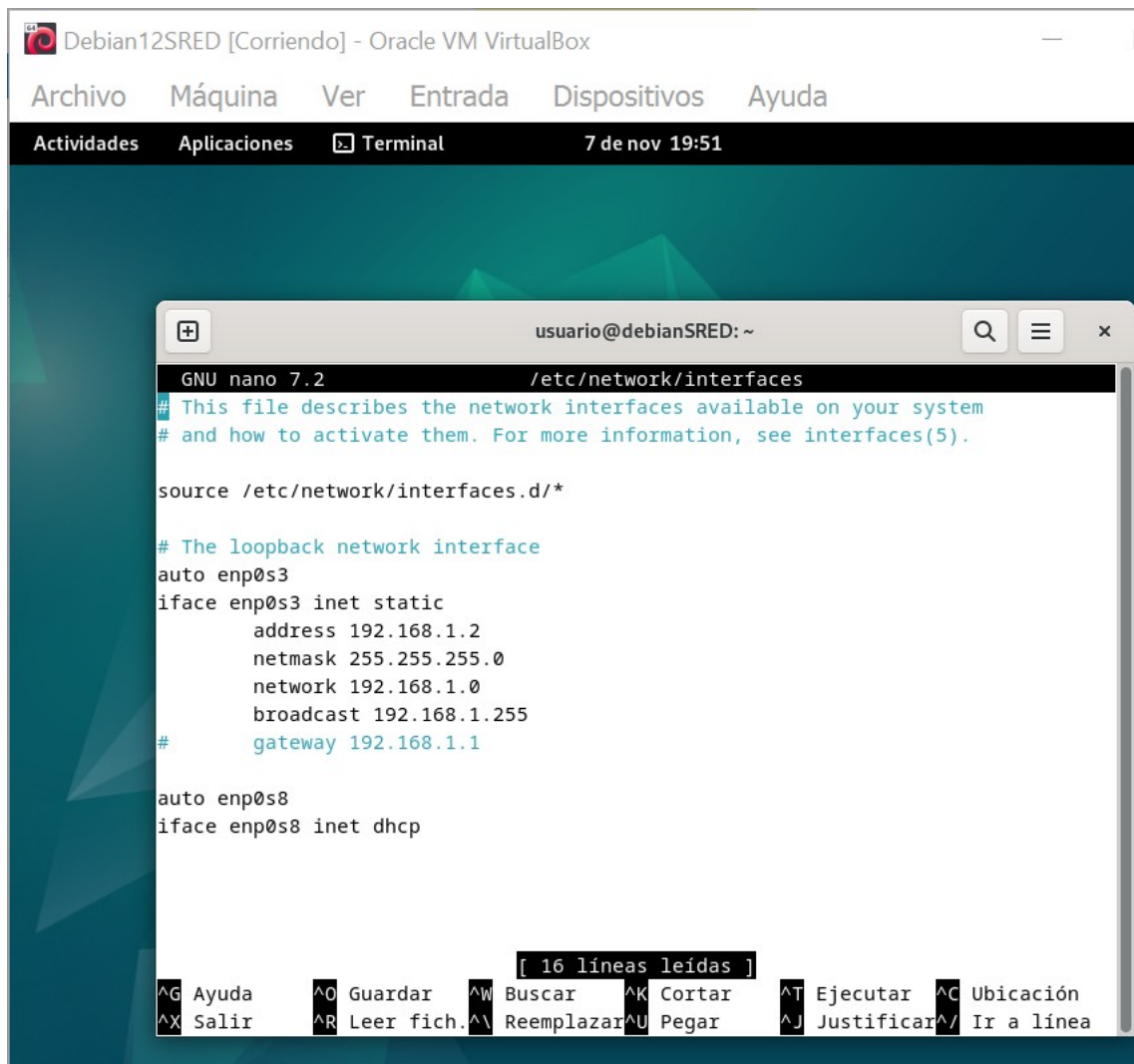
** server can't find jperalb.com: NXDOMAIN

root@debianSRED: /home/usuario#
```

Tras hacer la configuración, tendremos un servidor maestro, y por lo tanto, autoritario, para el dominio *jperalb.com*, incluyendo su zona inversa.

Para esta configuración y todas las demás, se va a trabajar en una única red de IP 192.168.1.0/24, y donde el router que da salida a internet es el 192.168.1.1.

Deshabilitamos NetworkManager, por si tenemos algún problema de conexión a la hora de configurar, y hacemos una copia del archivo a modificar `/etc/bind/named.conf.local`. Y en `/etc/network/interfaces` asignamos la ip correspondiente de la red, coincidiendo con ns1 del maestro.



```

Debian12SRED [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Aplicaciones  Terminal  7 de nov 19:51

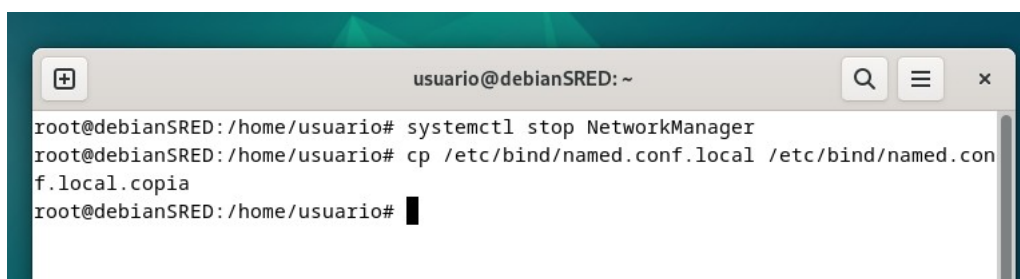
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto enp0s3
iface enp0s3 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    # gateway 192.168.1.1

auto enp0s8
iface enp0s8 inet dhcp

[ 16 líneas leídas ]
^G Ayuda  ^O Guardar  ^W Buscar  ^K Cortar  ^T Ejecutar  ^C Ubicación
^X Salir  ^R Leer fich.  ^\ Reemplazar  ^U Pegar  ^J Justificar  ^_ Ir a línea
  
```



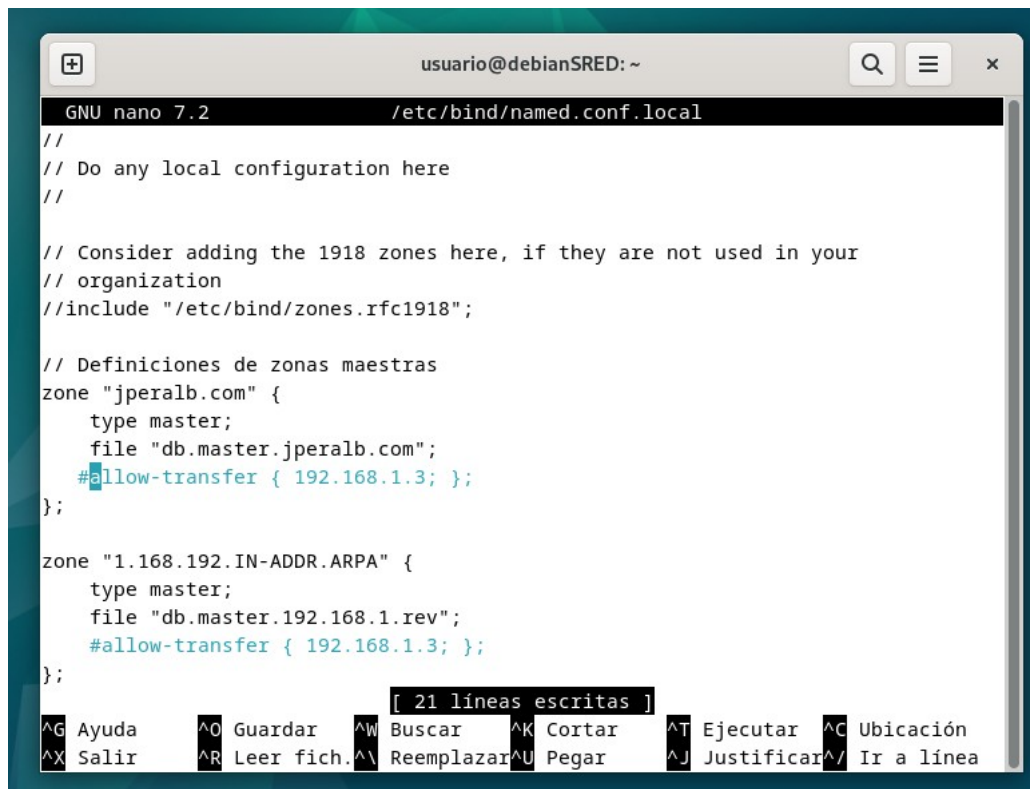
```

usuario@debianSRED: ~
root@debianSRED:/home/usuario# systemctl stop NetworkManager
root@debianSRED:/home/usuario# cp /etc/bind/named.conf.local /etc/bind/named.conf.local.copia
root@debianSRED:/home/usuario#
  
```

2.1 Configuración

Vamos a la ruta mencionada anteriormente y establecemos los siguientes datos.

Zona directa maestra y maestra inversa;



```

GNU nano 7.2 /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";

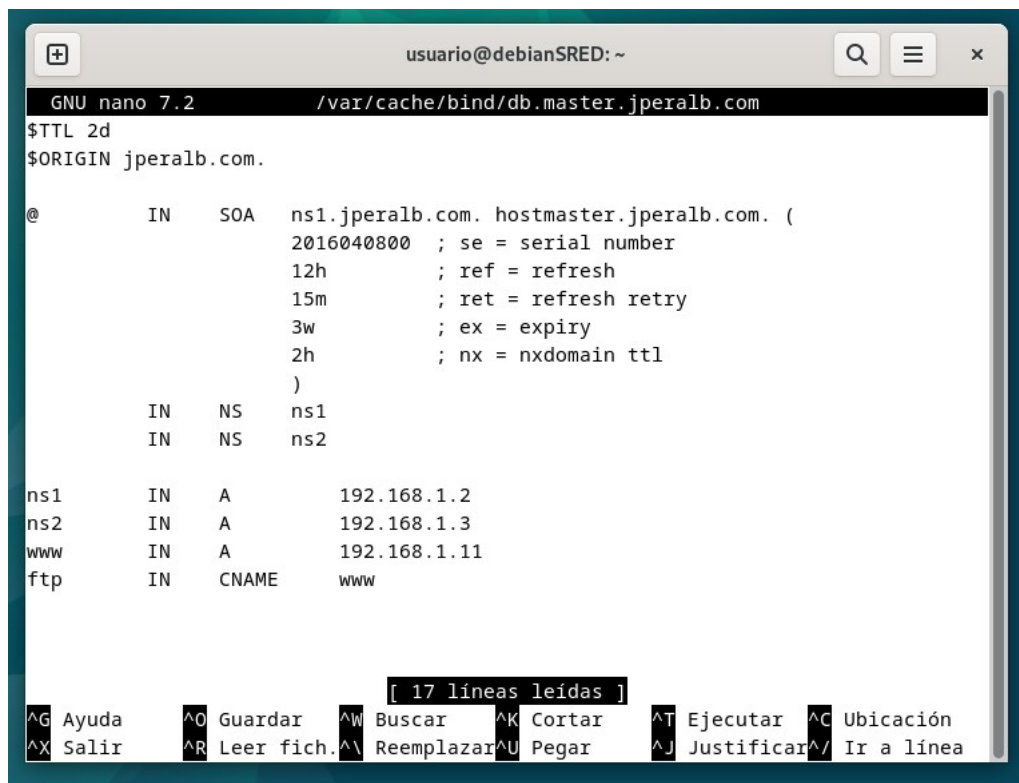
// Definiciones de zonas maestras
zone "jperalb.com" {
    type master;
    file "db.master.jperalb.com";
    #allow-transfer { 192.168.1.3; };
};

zone "1.168.192.IN-ADDR.ARPA" {
    type master;
    file "db.master.192.168.1.rev";
    #allow-transfer { 192.168.1.3; };
};

[ 21 líneas escritas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar      ^J Justificar ^_ Ir a línea
  
```

Una vez terminada la configuración de *named.conf*, lo que nos queda es crear los ficheros de zona (directo e inverso) con los RR necesarios (**Registros de recursos (RR)**): Ocupan una línea cada uno a excepción de las entradas que van entre paréntesis, las cuales pueden distribuirse en varias líneas. Sirven para definir características, propiedades y entidades del dominio).

Zona directa:



```

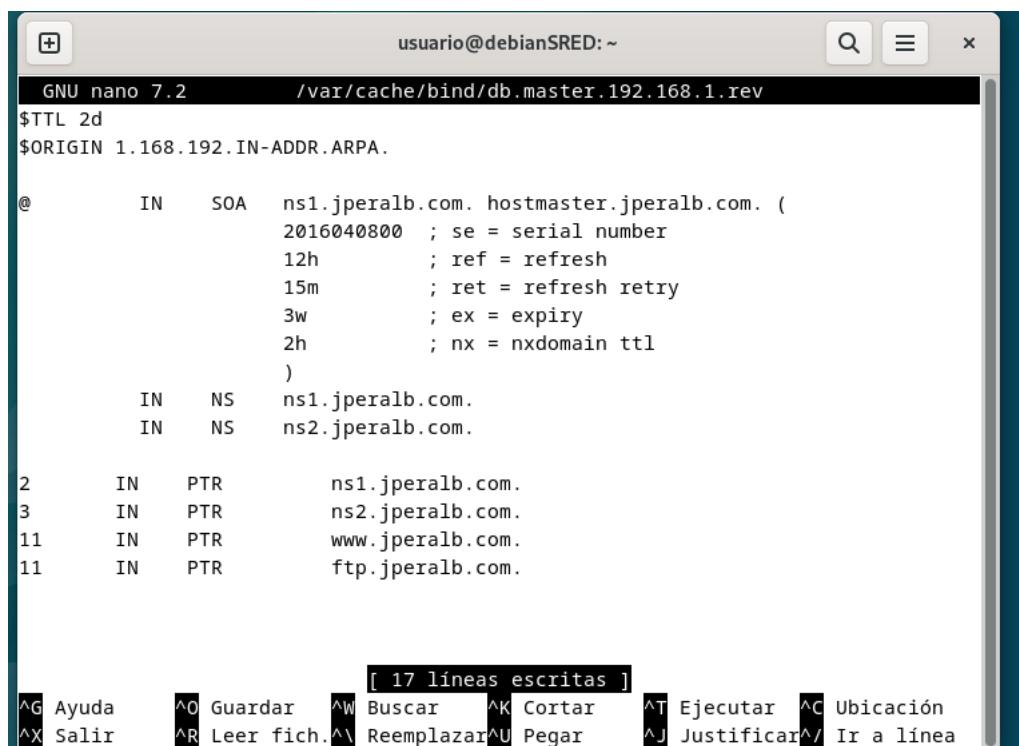
GNU nano 7.2 /var/cache/bind/db.master.jperralb.com
$TTL 2d
$ORIGIN jperralb.com.

@      IN      SOA     ns1.jperralb.com. hostmaster.jperralb.com. (
                                2016040800 ; se = serial number
                                12h         ; ref = refresh
                                15m         ; ret = refresh retry
                                3w          ; ex = expiry
                                2h         ; nx = nxdomain ttl
                                )
      IN      NS      ns1
      IN      NS      ns2

ns1     IN      A       192.168.1.2
ns2     IN      A       192.168.1.3
www     IN      A       192.168.1.11
ftp     IN      CNAME   www

[ 17 líneas leídas ]
^G Ayuda  ^O Guardar  ^W Buscar  ^K Cortar  ^T Ejecutar  ^C Ubicación
^X Salir  ^R Leer fich. ^\ Reemplazar ^U Pegar  ^J Justificar ^_ Ir a línea
  
```

Zona inversa:



```

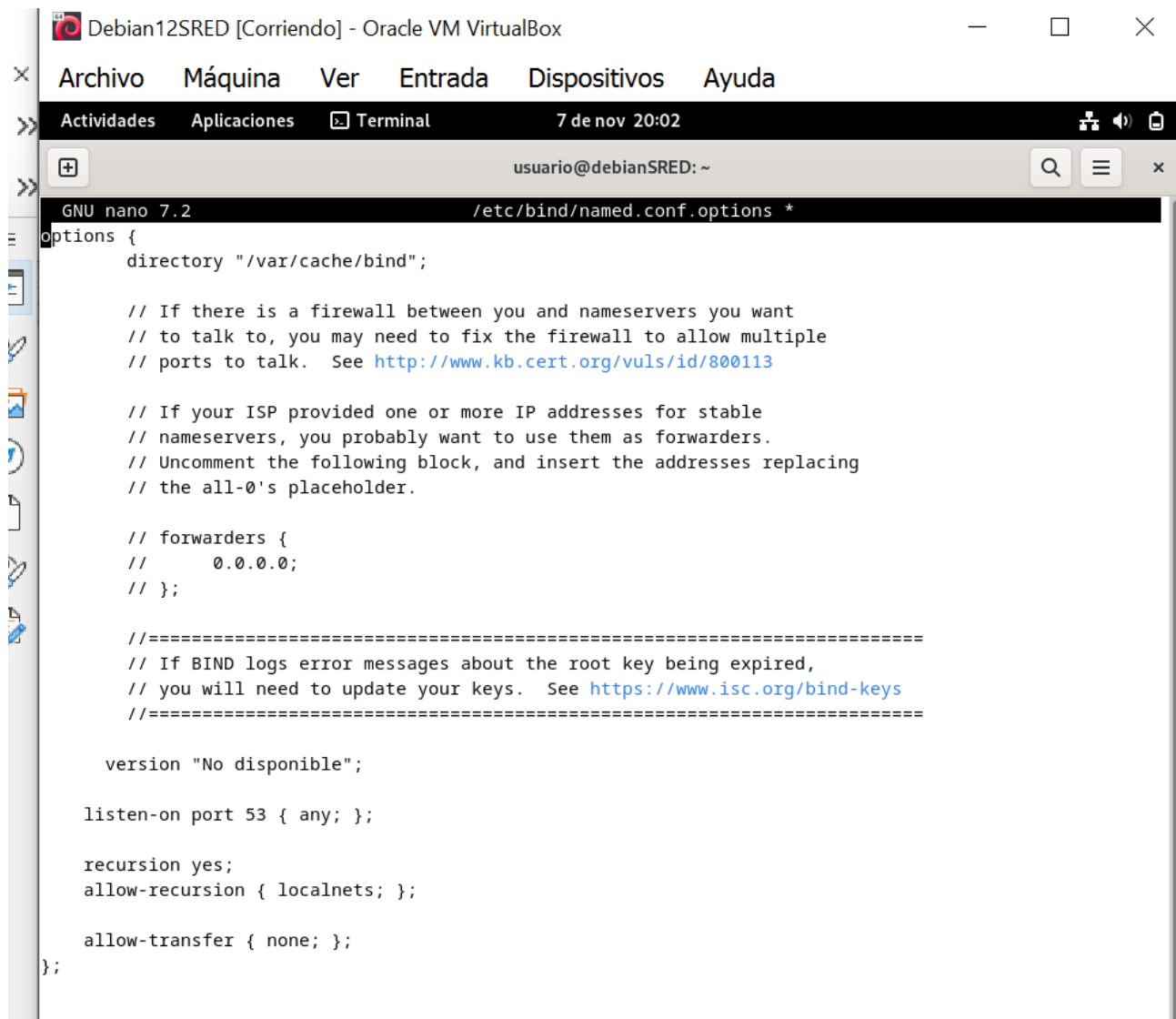
GNU nano 7.2 /var/cache/bind/db.master.192.168.1.rev
$TTL 2d
$ORIGIN 1.168.192.IN-ADDR.ARPA.

@      IN      SOA     ns1.jperralb.com. hostmaster.jperralb.com. (
                                2016040800 ; se = serial number
                                12h         ; ref = refresh
                                15m         ; ret = refresh retry
                                3w          ; ex = expiry
                                2h         ; nx = nxdomain ttl
                                )
      IN      NS      ns1.jperralb.com.
      IN      NS      ns2.jperralb.com.

2      IN      PTR     ns1.jperralb.com.
3      IN      PTR     ns2.jperralb.com.
11     IN      PTR     www.jperralb.com.
11     IN      PTR     ftp.jperralb.com.

[ 17 líneas escritas ]
^G Ayuda  ^O Guardar  ^W Buscar  ^K Cortar  ^T Ejecutar  ^C Ubicación
^X Salir  ^R Leer fich. ^\ Reemplazar ^U Pegar  ^J Justificar ^_ Ir a línea
  
```

Ahora configuramos las opciones del named, en el archivo `/etc/bind/named.conf.options`



```

Debian12SRED [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Aplicaciones  Terminal  7 de nov 20:02
usuario@debianSRED: ~
GNU nano 7.2 /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
    //=====

    version "No disponible";

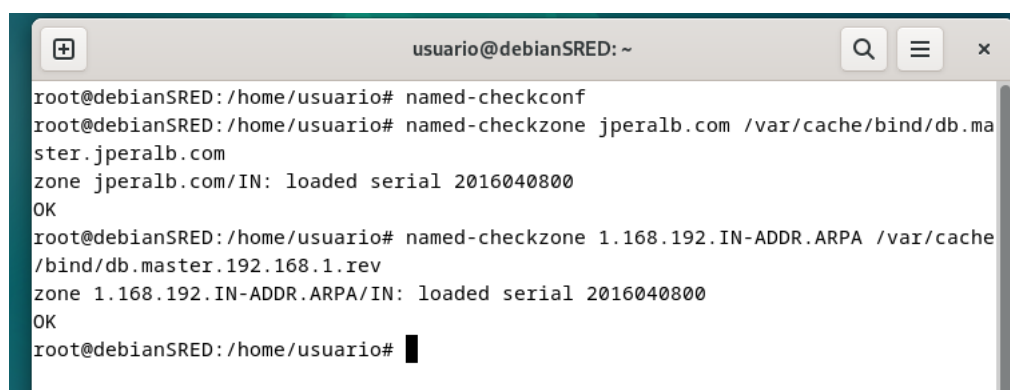
    listen-on port 53 { any; };

    recursion yes;
    allow-recursion { localnets; };

    allow-transfer { none; };
};

```

Vamos a ver si hay algún error en la sintaxis con el comando, primero un *named-checkconf* y luego un *named-checkzone*.



```

usuario@debianSRED: ~
root@debianSRED:/home/usuario# named-checkconf
root@debianSRED:/home/usuario# named-checkzone jperalb.com /var/cache/bind/db.master.jperalb.com
zone jperalb.com/IN: loaded serial 2016040800
OK
root@debianSRED:/home/usuario# named-checkzone 1.168.192.IN-ADDR.ARPA /var/cache/bind/db.master.192.168.1.rev
zone 1.168.192.IN-ADDR.ARPA/IN: loaded serial 2016040800
OK
root@debianSRED:/home/usuario#

```

2.2 Comprobación

Paramos el servicio named (puede capar nuestro dominio) y reiniciamos bind9. Y con el comando dig probamos que funcionan ambas zonas. Y ambas tienen respuesta (Answer section).

```

Debian12SRED [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Aplicaciones  Terminal  7 de nov 20:08
usuario@debianSRED: ~

root@debianSRED:/home/usuario# dig -x 192.168.1.11

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> -x 192.168.1.11
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33842
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 08264351b12bf47a01000000654a8af050199c459de71c60 (good)
;; QUESTION SECTION:
;11.1.168.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
11.1.168.192.IN-ADDR.ARPA. 172800 IN      PTR      ftp.jpéralb.com.
11.1.168.192.IN-ADDR.ARPA. 172800 IN      PTR      www.jpéralb.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Nov 07 20:07:28 CET 2023
;; MSG SIZE rcvd: 154

root@debianSRED:/home/usuario# dig ns2.jpéralb.com

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> ns2.jpéralb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32764
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

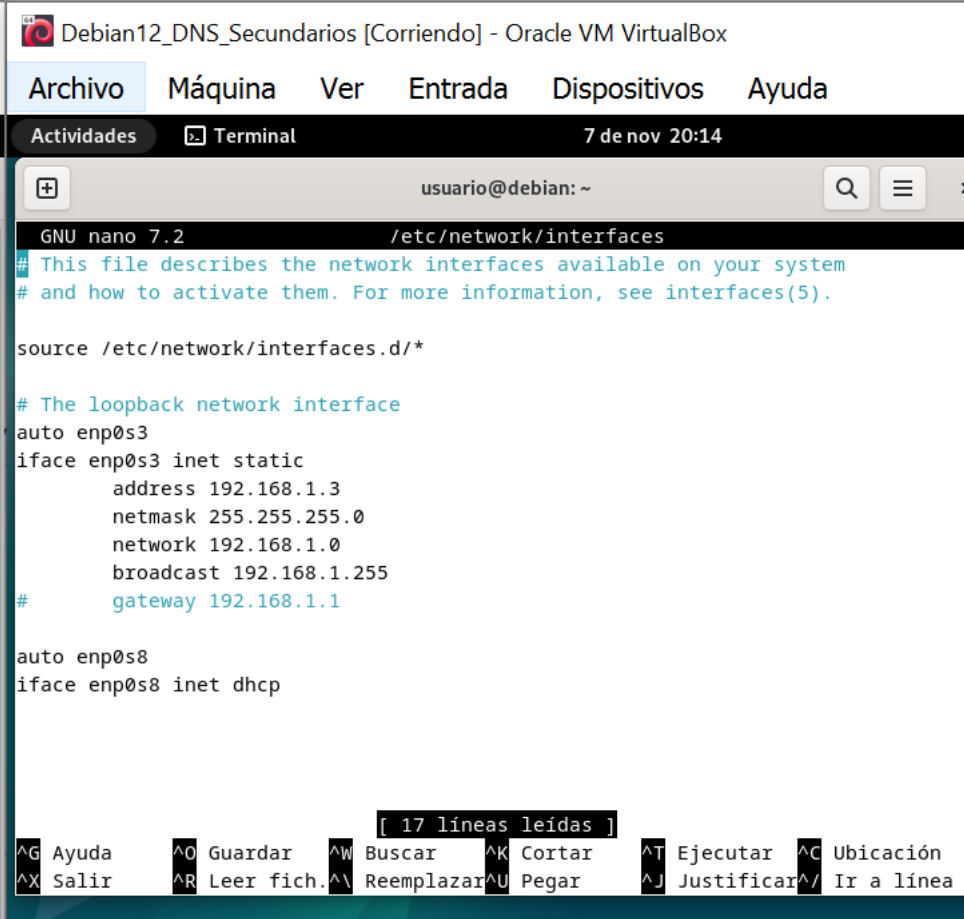
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 05f95d07baca89fd01000000654a8b182694dc725eebcb1d (good)
;; QUESTION SECTION:
;ns2.jpéralb.com.              IN      A

;; ANSWER SECTION:
ns2.jpéralb.com.      172800 IN      A      192.168.1.3

```

3. Configuración DNS Esclavo

Le asignaremos la ip 192.168.1.3 a la nueva MV que será la secundaria o esclava. Y cambiamos a nuestro servidor 127.0.0.1.



The screenshot shows a terminal window titled "Debian12_DNS_Secundarios [Corriendo] - Oracle VM VirtualBox". The terminal is running the nano text editor on the file `/etc/network/interfaces`. The current content of the file is as follows:

```
GNU nano 7.2 /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/*

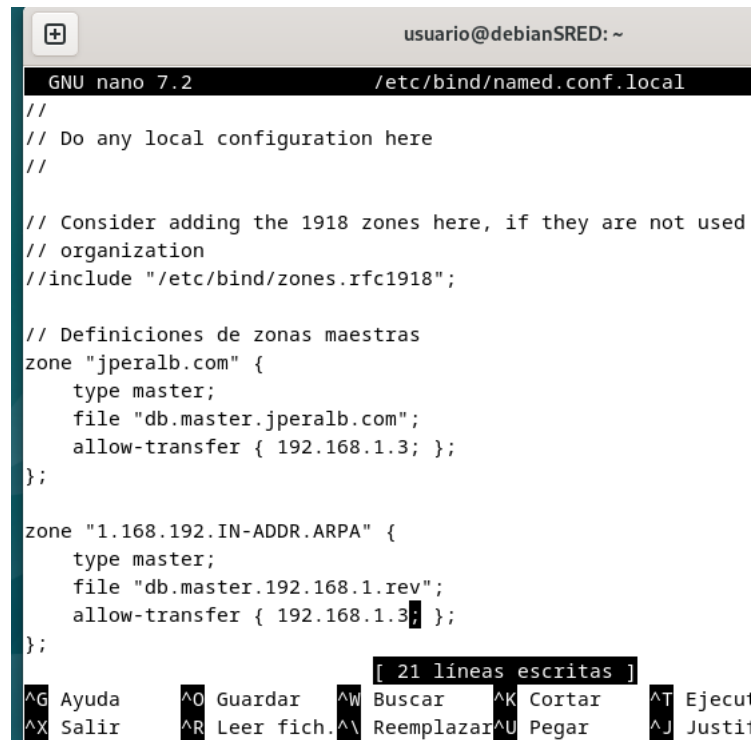
# The loopback network interface
auto enp0s3
iface enp0s3 inet static
    address 192.168.1.3
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
#     gateway 192.168.1.1

auto enp0s8
iface enp0s8 inet dhcp
```

At the bottom of the terminal, there is a status bar showing "[17 líneas leídas]" and a list of keyboard shortcuts for nano:

^G Ayuda	^O Guardar	^W Buscar	^K Cortar	^T Ejecutar	^C Ubicación
^X Salir	^R Leer fich.	^_\ Reemplazar	^U Pegar	^J Justificar	^_ Ir a línea

Y por último, en el fichero `/etc/bind/named.conf.local`, del master activamos el `allow-transfer` para añadir ese dns secundario, el cual servirá de unión entre el master y el esclavo.

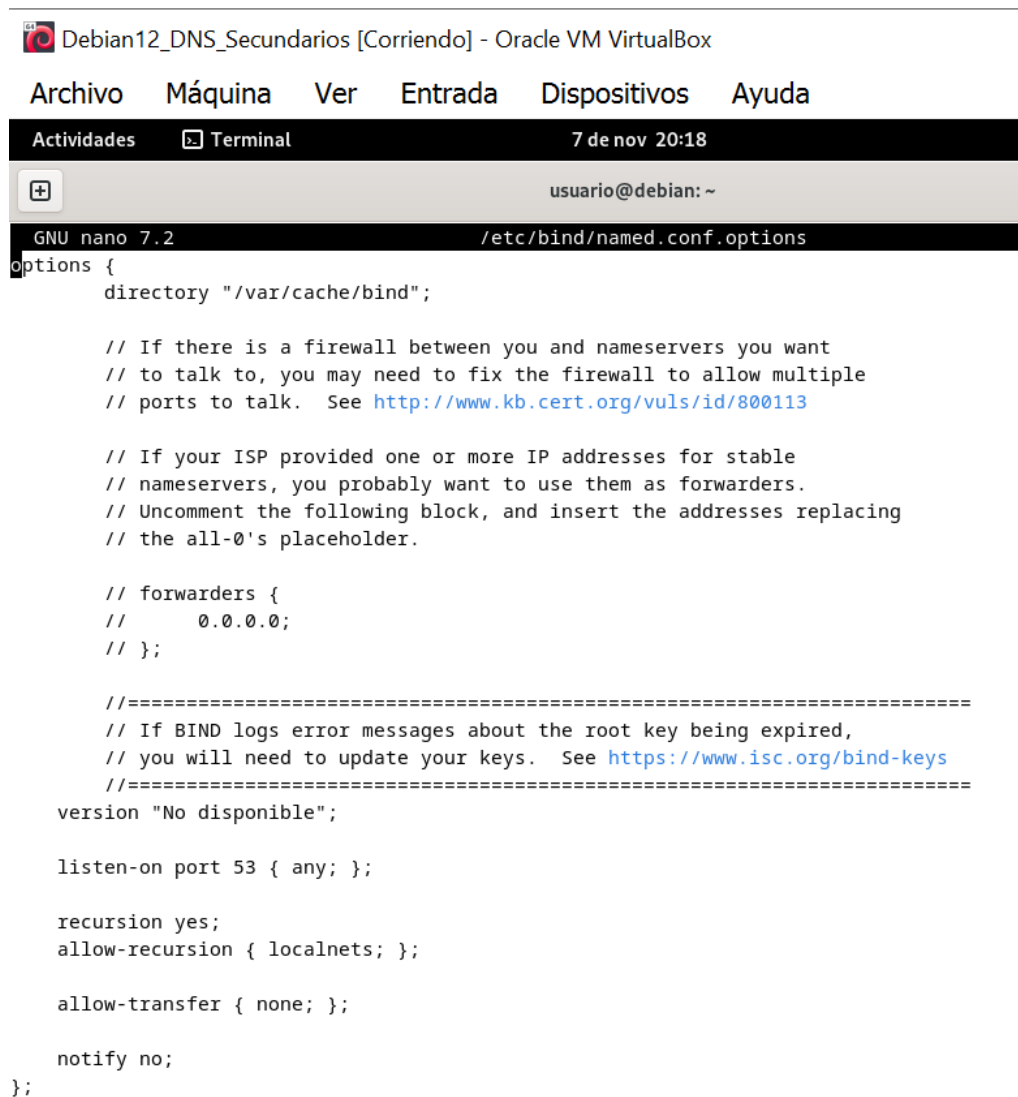


```
GNU nano 7.2 /etc/bind/named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used
// organization
//include "/etc/bind/zones.rfc1918";
// Definiciones de zonas maestras
zone "jperalb.com" {
    type master;
    file "db.master.jperalb.com";
    allow-transfer { 192.168.1.3; };
};
zone "1.168.192.IN-ADDR.ARPA" {
    type master;
    file "db.master.192.168.1.rev";
    allow-transfer { 192.168.1.3; };
};
[ 21 líneas escritas ]
^G Ayuda  ^O Guardar  ^W Buscar  ^K Cortar  ^T Ejecut
^X Salir   ^R Leer fich. ^\ Reemplazar ^U Pegar    ^J Justi
```

3.1 Configuración

Una vez tenemos la nueva MV procedemos a instalar el bind9, y configuramos el fichero `named.conf.options` quedando asi:

- Directorio para las rutas relativas: `/var/cache/bind`.
- No se dará información sobre la versión de BIND.
- El servidor escuchará por todas sus tarjetas por el puerto 53.
- El servidor funcionará como caché DNS para las redes a las que está conectado.
- Se prohibirán las transferencias de zona.
- No se prohibirán los mensajes NOTIFY.



```

Debian12_DNS_Secundarios [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  7 de nov 20:18
usuario@debian: ~
GNU nano 7.2 /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
    //=====
    version "No disponible";

    listen-on port 53 { any; };

    recursion yes;
    allow-recursion { localnets; };

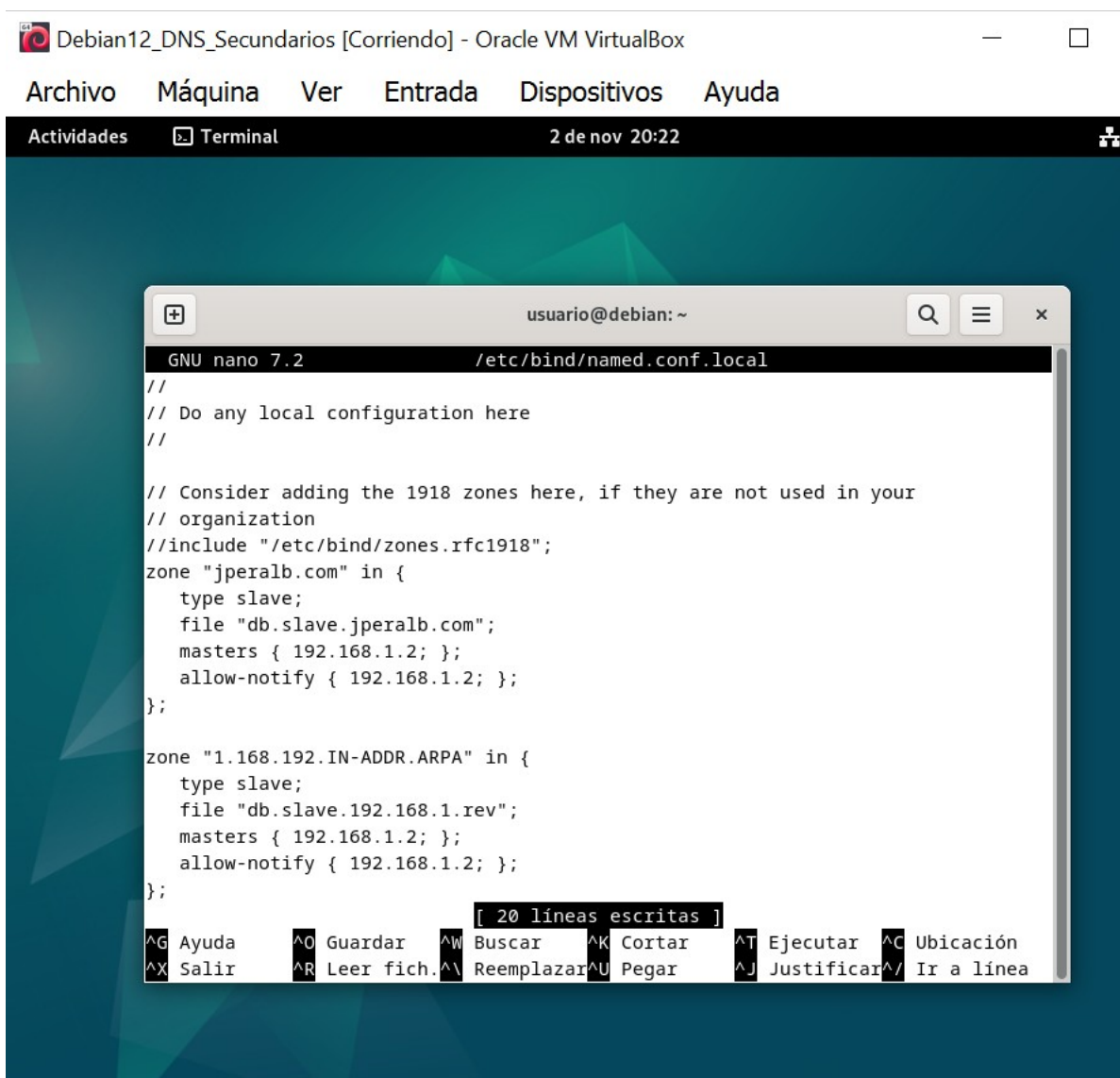
    allow-transfer { none; };

    notify no;
};

```


Definiremos ahora la zona esclava para el dominio *jperalb.com* con la cláusula *zone* en el fichero */etc/bind/named.conf.local*. La propiedades de esta zona son;

- Zona esclava.
- El fichero de zona será */var/cache/bind/db.slave.jperalb.com*.
- Las peticiones de transferencia de zona se realizarán únicamente al servidor maestro de dirección IP *192.168.1.2*.
- Por seguridad, solo aceptaremos mensajes NOTIFY del servidor maestro



The screenshot shows a terminal window titled "Debian12_DNS_Secundarios [Corriendo] - Oracle VM VirtualBox". The terminal is running the nano text editor on the file `/etc/bind/named.conf.local`. The configuration defines two slave zones. The first zone is for `jperalb.com`, with its database file at `db.slave.jperalb.com`, master IP at `192.168.1.2`, and `allow-notify` set to `{ 192.168.1.2; }`. The second zone is for `1.168.192.IN-ADDR.ARPA`, with its database file at `db.slave.192.168.1.rev`, master IP at `192.168.1.2`, and `allow-notify` set to `{ 192.168.1.2; }`. The terminal status bar indicates "[20 líneas escritas]" and shows various keyboard shortcuts for editing.

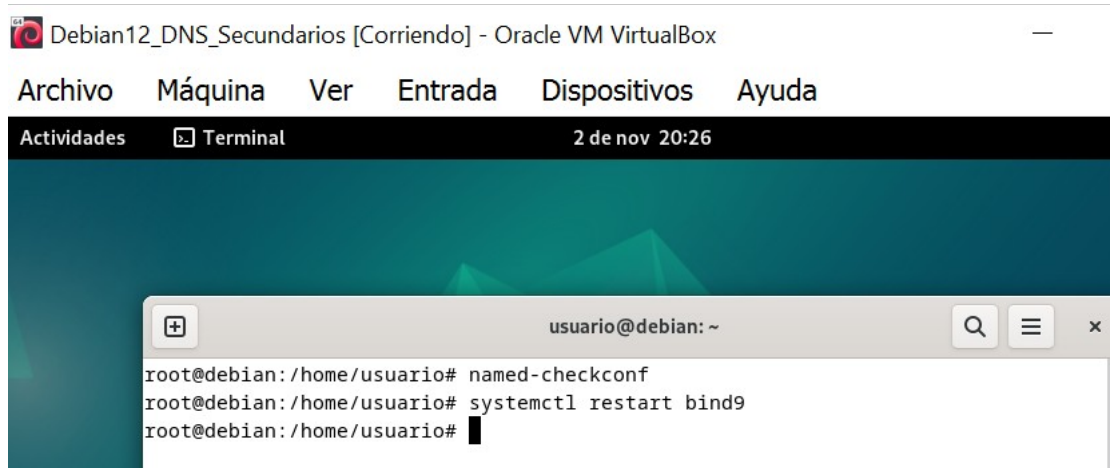
```
GNU nano 7.2 /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "jperalb.com" in {
    type slave;
    file "db.slave.jperalb.com";
    masters { 192.168.1.2; };
    allow-notify { 192.168.1.2; };
};

zone "1.168.192.IN-ADDR.ARPA" in {
    type slave;
    file "db.slave.192.168.1.rev";
    masters { 192.168.1.2; };
    allow-notify { 192.168.1.2; };
};

[ 20 líneas escritas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar      ^J Justificar ^_ Ir a línea
```

Hacemos named-checkconf, y como todo parece estar correcto, reiniciamos el servicio bind9, tanto en el master como en el esclavo.



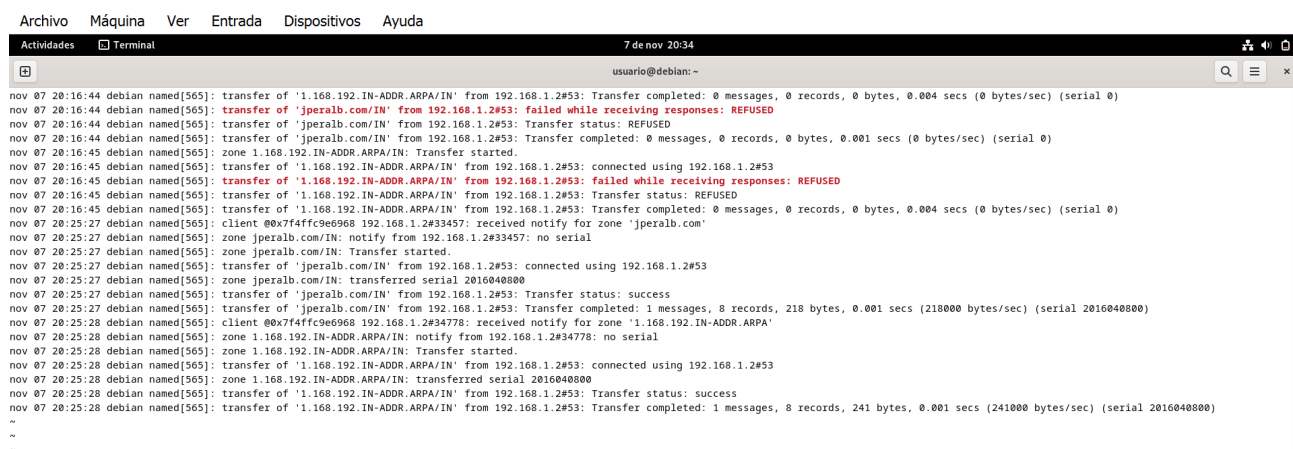
```

Debian12_DNS_Secundarios [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  2 de nov 20:26

usuario@debian: ~
root@debian:/home/usuario# named-checkconf
root@debian:/home/usuario# systemctl restart bind9
root@debian:/home/usuario#

```

Tras hacerlo, hacemos un journalctl -b -u named en el esclavo y vemos como se produce la transferencia (Las que están mas abajo, la última configuración)



```

Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  7 de nov 20:34

usuario@debian: ~
nov 07 20:16:44 debian named[565]: transfer of '1.168.192.IN-ADDR.ARPA/IN' from 192.168.1.2#53: Transfer completed: 0 messages, 0 records, 0 bytes, 0.004 secs (0 bytes/sec) (serial 0)
nov 07 20:16:44 debian named[565]: transfer of 'jperalb.com/IN' from 192.168.1.2#53: failed while receiving responses: REFUSED
nov 07 20:16:44 debian named[565]: transfer of 'jperalb.com/IN' from 192.168.1.2#53: Transfer status: REFUSED
nov 07 20:16:44 debian named[565]: transfer of 'jperalb.com/IN' from 192.168.1.2#53: Transfer completed: 0 messages, 0 records, 0 bytes, 0.001 secs (0 bytes/sec) (serial 0)
nov 07 20:16:45 debian named[565]: zone 1.168.192.IN-ADDR.ARPA/IN: Transfer started.
nov 07 20:16:45 debian named[565]: transfer of '1.168.192.IN-ADDR.ARPA/IN' from 192.168.1.2#53: connected using 192.168.1.2#53
nov 07 20:16:45 debian named[565]: transfer of '1.168.192.IN-ADDR.ARPA/IN' from 192.168.1.2#53: failed while receiving responses: REFUSED
nov 07 20:16:45 debian named[565]: transfer of '1.168.192.IN-ADDR.ARPA/IN' from 192.168.1.2#53: Transfer status: REFUSED
nov 07 20:25:27 debian named[565]: Client 00x7f4ffc9e9608 192.168.1.2#33457: received notify for zone 'jperalb.com'
nov 07 20:25:27 debian named[565]: zone jperalb.com/IN: notify from 192.168.1.2#33457: no serial
nov 07 20:25:27 debian named[565]: zone jperalb.com/IN: Transfer started.
nov 07 20:25:27 debian named[565]: transfer of 'jperalb.com/IN' from 192.168.1.2#53: connected using 192.168.1.2#53
nov 07 20:25:27 debian named[565]: zone jperalb.com/IN: transferred serial 2016040800
nov 07 20:25:27 debian named[565]: transfer of 'jperalb.com/IN' from 192.168.1.2#53: Transfer status: success
nov 07 20:25:27 debian named[565]: transfer of 'jperalb.com/IN' from 192.168.1.2#53: Transfer completed: 1 messages, 8 records, 218 bytes, 0.001 secs (218000 bytes/sec) (serial 2016040800)
nov 07 20:25:28 debian named[565]: client 00x7f4ffc9e9608 192.168.1.2#34778: received notify for zone '1.168.192.IN-ADDR.ARPA'
nov 07 20:25:28 debian named[565]: zone 1.168.192.IN-ADDR.ARPA/IN: notify from 192.168.1.2#34778: no serial
nov 07 20:25:28 debian named[565]: zone 1.168.192.IN-ADDR.ARPA/IN: Transfer started.
nov 07 20:25:28 debian named[565]: transfer of '1.168.192.IN-ADDR.ARPA/IN' from 192.168.1.2#53: connected using 192.168.1.2#53
nov 07 20:25:28 debian named[565]: zone 1.168.192.IN-ADDR.ARPA/IN: transferred serial 2016040800
nov 07 20:25:28 debian named[565]: transfer of '1.168.192.IN-ADDR.ARPA/IN' from 192.168.1.2#53: Transfer status: success
nov 07 20:25:28 debian named[565]: transfer of '1.168.192.IN-ADDR.ARPA/IN' from 192.168.1.2#53: Transfer completed: 1 messages, 8 records, 241 bytes, 0.001 secs (241000 bytes/sec) (serial 2016040800)
~
~

```

Ahora lo comprobaremos con el dig.

3.2 Comprobación

```

Debian12_DNS_Secundarios [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  7 de nov 20:39
usuario@debian: ~
root@debian:/home/usuario# dig @192.168.1.2 jperalb.com AXFR

;<<>> DiG 9.18.19-1~deb12u1-Debian <<>> @192.168.1.2 jperalb.com AXFR
; (1 server found)
;; global options: +cmd
jperalb.com.      172800  IN      SOA      ns1.jperalb.com. hostmaster.jperalb.com. 2016040800 4320
0 900 1814400 7200
jperalb.com.      172800  IN      NS       ns1.jperalb.com.
jperalb.com.      172800  IN      NS       ns2.jperalb.com.
ftp.jperalb.com.  172800  IN      CNAME    www.jperalb.com.
ns1.jperalb.com.  172800  IN      A        192.168.1.2
ns2.jperalb.com.  172800  IN      A        192.168.1.3
www.jperalb.com.  172800  IN      A        192.168.1.11
jperalb.com.      172800  IN      SOA      ns1.jperalb.com. hostmaster.jperalb.com. 2016040800 4320
0 900 1814400 7200
;; Query time: 0 msec
;; SERVER: 192.168.1.2#53(192.168.1.2) (TCP)
;; WHEN: Tue Nov 07 20:39:37 CET 2023
;; XFR size: 8 records (messages 1, bytes 257)
root@debian:/home/usuario#

```

```

Debian12_DNS_Secundarios [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  7 de nov 20:41
usuario@debian: ~
oot@debian:/home/usuario# dig @192.168.1.2 www.jperalb.com

<<>> DiG 9.18.19-1~deb12u1-Debian <<>> @192.168.1.2 www.jperalb.com
(1 server found)
; global options: +cmd
; Got answer:
; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 31743
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

; OPT PSEUDOSECTION:
EDNS: version: 0, flags:; udp: 1232
COOKIE: 8b8a53503d223a0f01000000654a92cf250fbf6ec4dff3cf (good)
; QUESTION SECTION:
www.jperalb.com.      IN      A

; ANSWER SECTION:
www.jperalb.com.      172800  IN      A        192.168.1.11

; Query time: 4 msec
; SERVER: 192.168.1.2#53(192.168.1.2) (UDP)
; WHEN: Tue Nov 07 20:41:02 CET 2023
; MSG SIZE rcvd: 88
oot@debian:/home/usuario#

```