DNS EN LINUX. SERVIDOR ESCLAVO O SECUNDARIO

Hamza Akdi

03/11/2025

Índice:

PARTE 1: SERVIDOR ESCLAVO O SECUNDARIO

En este apartado debes conseguir que un servidor Bind instalado en otra máquina Linux trabaje como secundario para tu zona (asir20.net o isaacbvgf.net). Para ello debes (forma rápida sugerida, **documenta** cada apartado):

Clonar tu máquina Linux.

Cambiar el nombre de la máquina: slave20.asir20.net o slave20.isaacbvgf.net

Comprobar que hay conectividad entre el servidor maestro (el que tenías) y el esclavo (el que acabas de clonar).

Comenzaremos con la clonación de nuestra maquina servidora DNS, la cual cambiaremos de nombre a **slave.hamza.net** en la siguiente ruta:

Con este comando cambiaremos el nombre de host de nuestra máquina.

```
root@hamza:/home/hamza# sudo nano /etc/hostname
```

```
  GNU nano 8.4                    /etc/hostname *
slave
```

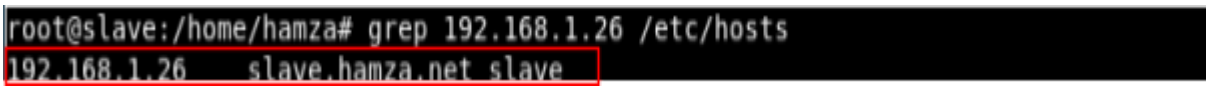
(Cambio de nombre de host)

En la máquina clonada: Asignaremos la IP estática **192.168.1.23**. Cambiaremos el nombre a **slave.hamza.net.**

```
  GNU nano 8.4                          /etc/hosts *
127.0.0.1       localhost
192.168.1.26    slave.hamza.net slave

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

(Configuración de IP y asignación de nombre del esclavo)

Con el siguiente comando confirmaremos los cambios realizados en el fichero de configuración anterior:



(Confirmación de los cambios del fichero)

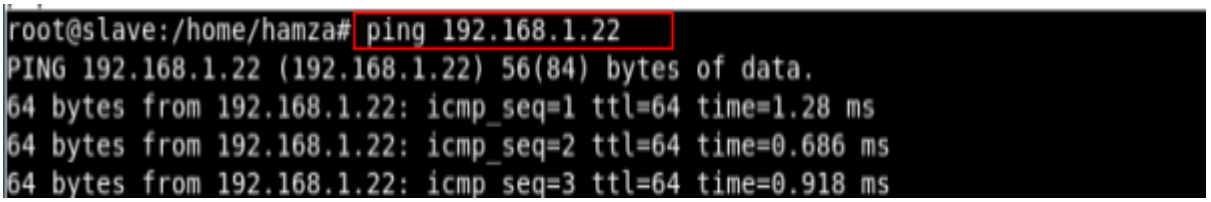
Al ver que los archivos son correctos, usaremos **hostnamectl** para aplicar el cambio en el sistema sin necesidad de reiniciar la máquina, aplicando el nombre en la configuración del kernel.

Reiniciamos el servicio y verificaremos que se ha hecho correctamente con los siguientes comandos:

(Confirmación de cambio de nombre del host)

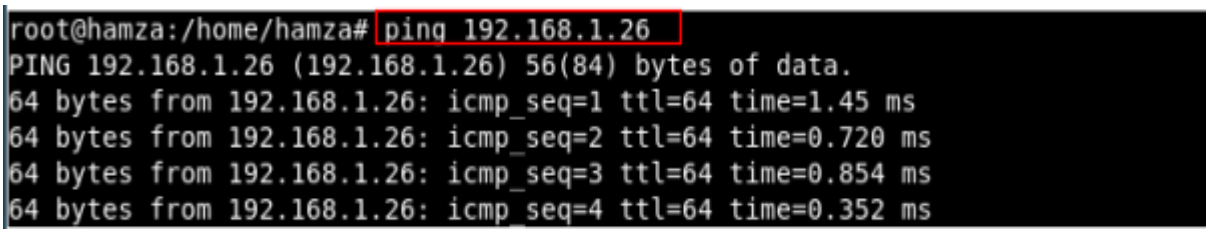
Ahora comprobaremos que la conexión este el Maestro y el Esclavo. Este paso es crucial, ya que si el Maestro (192.168.1.22) y el Esclavo (192.168.1.26) no se comunican, la transferencia de zona fallará.

Primero haremos un ping del **esclavo al maestro**, confirmando que hay conexión.



(Ping de máquina Esclavo a máquina Maestro)

Ping maquina **Maestro a máquina Esclavo**, confirmando la interconexión entre ambas:



(Ping Maestro a Esclavo)

En el secundario:

- Borrar el fichero de zona /etc/bind/db.isaacbvgf.net o /etc/bind/db.asir20.net

Con el siguiente comando borraremos todo fichero de zona del servidor Esclavo:

```
root@slave:/home/hamza# sudo rm /etc/bind/db.hamza.net
```

- Modificar el fichero named.conf.local (para que trabaje como esclavo y para que sepa a quién debe solicitar el fichero de zona).

En el servidor esclavo, modificaremos el fichero de configuración **named.conf.local** de la siguiente manera, asumiendo que el servidor esclavo será secundario para la zona directa:

```
  GNU nano 8.4                /etc/bind/named.conf.local *
// Do any local configuration here
//
// Esta es la zona directa: hamza.net
zone "hamza.net" {
    type slave;
    file "db.hamza.net";
    masters { 192.168.1.22; }; // IP del Servidor Maestro
};
```

(Configuración del fichero named.conf.local del Servidor Esclavo)

Una vez que guardemos este archivo en **el Esclavo**, debemos volver al **Servidor Maestro** (192.168.1.22) para autorizar la transferencia de zona y luego reiniciar ambos servicios para que se inicie la descarga.

En el primario:

- Modificar el fichero de zona para incluir el nuevo servidor.

Ya configurado el archivo Esclavo, iremos a la ruta **/etc/bind/named.conf.local** de nuestro **servidor Maestro** y la configuraremos de la siguiente manera. El apartado

allow-transfer, indica al **Servidor Maestro** quién está autorizado a solicitar y recibir una copia completa del fichero de zona. Donde indicaremos el **servidor Esclavo** (192.168.1.26)**.**

(Configuración del fichero named.conf.local Servidor Maestro)

Al realizar cada configuración de ficheros, reiniciaremos los servicios con el siguiente comando:

```
root@slave:/home/hamza# sudo systemctl restart bind9
```

```
root@hamza:/home/hamza# sudo systemctl restart bind9
```

Es importante que el secundario no tenga ficheros de zona: debe descargarlos al arrancar por primera vez. Investiga dónde se descargan y con qué nombre. Muestra un listado del directorio.

La ruta estándar donde BIND guarda automáticamente los ficheros de zona transferidos es: /var/cache/bind/

Este directorio se usa para almacenar datos dinámicos que cambian con frecuencia, como los ficheros de zona que se actualizan y la caché de consultas.

El fichero de zona se ha descargado del servidor primario y se almacena en el directorio de caché de BIND, donde se puede observar el fichero **db.hamza.net.**

```
root@slave:/home/hamza# ls -l /var/cache/bind/
total 12
-rw-r--r-- 1 bind bind  673 nov  3 15:25 db.hamza.net
-rw-r--r-- 1 bind bind 1411 nov  3 15:25 managed-keys.bind
-rw-r--r-- 1 bind bind 3020 nov  3 15:24 managed-keys.bind.jnl
```

(Directorio de caché de BIND)

Muestra una captura del fichero descargado. ¿Es igual que el del maestro?

Utilizaremos el siguiente comando para descargar el fichero de zona:

```
root@slave:/home/hamza# sudo cat /var/cache/bind/db.hamza.net
```

Ya descargado el fichero de zona por el **servidor esclavo desde el maestro**. Al intentar mostrar su contenido con **cat**, se observan caracteres binarios, ya que **BIND** almacena los ficheros descargados en un formato binario optimizado. A pesar de que no es texto plano, se confirma que el fichero es lógicamente idéntico al del maestro.

```
root@slave:/home/hamza# sudo cat /var/cache/bind/db.hamza.net
@\U     :@
         hamzanet4ns1hamzanetadminhamzanetx@@W :@Q@$@  :@3     :@
                                                          hamzanet
mailhamzanet0   :@
                 hamzanetns1hamzanet(  :@dbhamzanet@@j?4       :@docshamzanetdb
hamzanet:       :@ftphamzanet   servidor1hamzanet*      :@mailhamzanet@@7)     :
@ns1hamzanet@@/ :@      servidor1hamzanet@@j=/  :@      servidor2hamzanet@@j>) :
@vpnhamzanet@@j@8       :@web-rrhamzanet@@@@@@@@@)      :@wwwhamzanet@@root@slav
```

(Descarga de fichero de zona en servidor Esclavo)

Investiga qué son las notificaciones. ¿Están activadas por defecto en el maestro? Si no, actívalas.

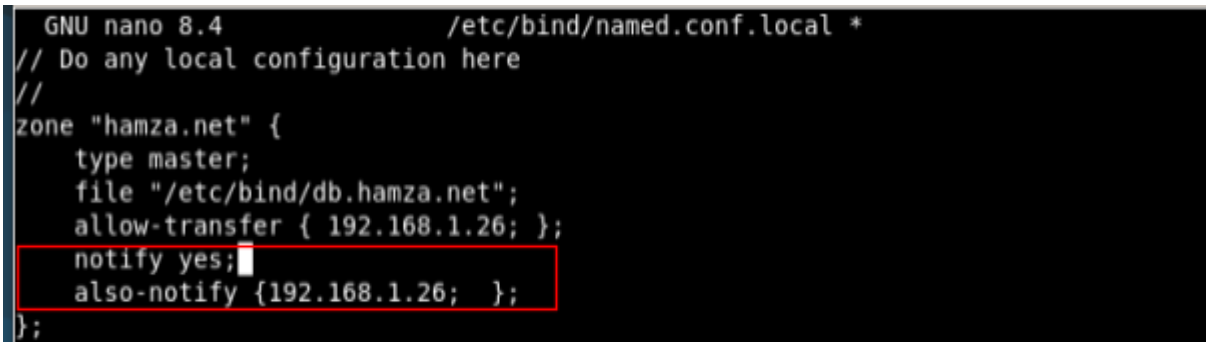
Las notificaciones DNS son un mecanismo de comunicación utilizado por el servidor DNS **Maestro** para informar inmediatamente a sus servidores **Esclavos** de que el fichero de zona ha sido actualizado y necesita ser transferido.

Con el objetivo de reducir el tiempo de propagación de cambios. Sin notificaciones, el esclavo tendría que esperar al tiempo definido en el parámetro "**Refresh".** Cuando

el **Maestro** detecta que su número de **Serial** ha incrementado, envía un mensaje **“NOTIFY”** a sus esclavos.

Al recibir la notificación, el **Esclavo** inmediatamente consulta al **Maestro** el **número de Serial**. Si el **Serial** del **Maestro** es mayor, el **Esclavo** inicia una transferencia de zona incremental.

Sí, las **notificaciones están activadas** por defecto en el servidor BIND. Si tuviéramos que activarlas manualmente, usarías la directiva **notify** en el bloque **options** o dentro de la declaración de la zona de la siguiente manera:



(Fichero de configuración named.conf.local activando notificaciones)

Explica qué tipos de transferencia de ficheros de zona hay. ¿Qué puerto se utiliza para las transferencias de zona?

La transferencia de ficheros de zona es el mecanismo que permite a un servidor DNS Secundario (Esclavo) replicar los datos de una zona desde un servidor Primario (Maestro).

Existen dos tipos principales de transferencia de zona en DNS, diseñados para optimizar la velocidad y el uso de ancho de banda:

- Transferencia Completa de Zona (AXFR): Transfiere **todo el contenido** del fichero de zona, desde el Servidor Maestro al Servidor Esclavo, independientemente de la cantidad de cambios realizados. Se utiliza la primera vez que un servidor esclavo solicita la zona, o si la transferencia incremental (IXFR) falla.

- Transferencia Incremental de Zona (IXFR): Transfiere **solo los cambios** que se han realizado en la zona desde la última transferencia exitosa. Se utiliza después de la transferencia inicial, cuando el número de

Serial del Maestro es mayor que el Serial del Esclavo. Esto ahorra ancho de banda y tiempo de procesamiento.

El puerto estándar utilizado para las transferencias de zona es el puerto **TCP 53.** Se utiliza el puerto **UDP 53** para las consultas normales y **TCP 53** para tareas más grandes que requieren fiabilidad y verificación de la transferencia de datos, como las transferencias de zona y las comunicaciones seguras.

Realiza consultas (cuatro al menos) al servidor esclavo. Realiza cambios en el fichero de zona del servidor maestro: añade un nuevo registro. No modifiques el campo serial del SOA. Reinicia el servidor primario y luego el secundario y comprueba el fichero de zona en el secundario: ¿se ha actualizado?

Realizaremos cuatro consultas al servidor esclavo (192.168.1.26) para confirmar que cargó correctamente la zona y está respondiendo como autoridad.

Consultas Iniciales al Servidor Esclavo:

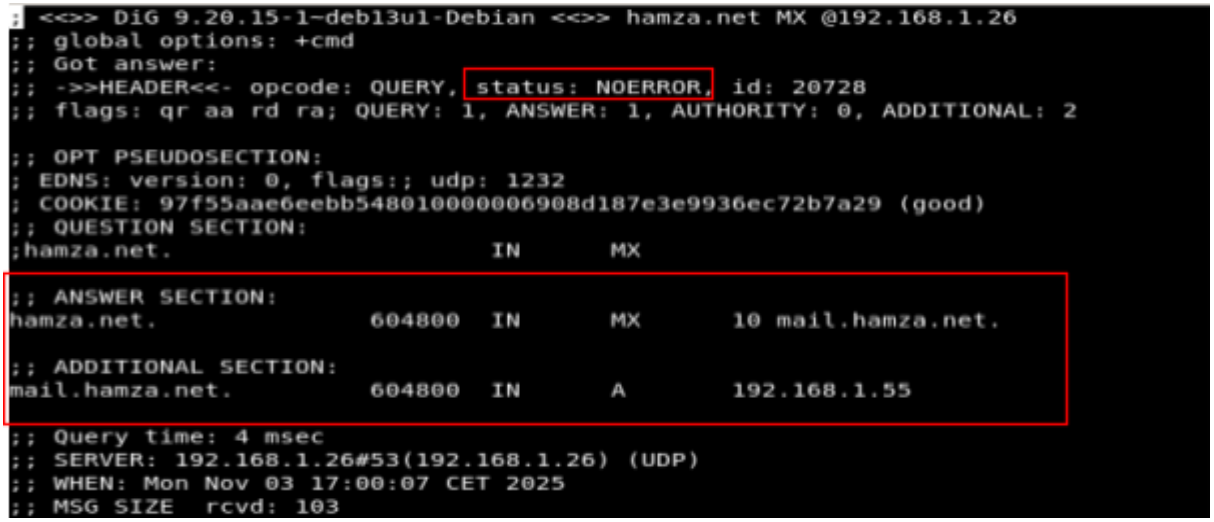
Primera consulta **al Alias**, comprando que resuelve correctamente el alias **www.**

```
root@hamza:/home/hamza# nslookup www.hamza.net 192.168.1.26
Server:         192.168.1.26
Address:        192.168.1.26#53

Name:   www.hamza.net
Address: 192.168.1.23
```

(Consulta al Alias del servidor Esclavo)

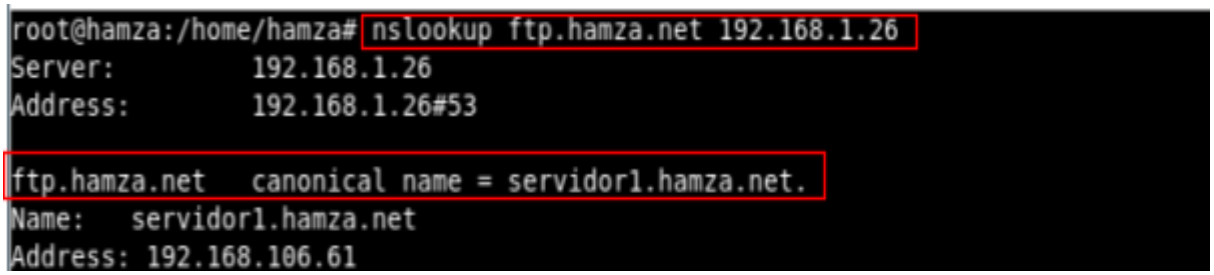
Segunda consulta (MX), comprobando que conoce el registro de correo:

```
root@hamza:/home/hamza# dig hamza.net MX @192.168.1.26
```



(Consulta al mail del servidor Esclavo)

Tercera consulta al **CNAME**, dando a ver que el **servidor Esclavo** resuelve el alias **ftp.**



(Consulta al CNAME del servidor Esclavo)

Cuarta consulta a **NS**, donde podemos ver que el **servidor Esclavo** confirma que **ns1.hamza.net es la autoridad**.

```
; <<>> DiG 9.20.15-1~deb13u1-Debian <<>> hamza.net NS @192.168.1.26
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3032
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3bac29a07453a371010000006908d2f65ffd79b8a7bc6255 (good)
;; QUESTION SECTION:
;hamza.net.                     IN      NS

;; ANSWER SECTION:
hamza.net.              604800  IN      NS      ns1.hamza.net.

;; ADDITIONAL SECTION:
ns1.hamza.net.          604800  IN      A       192.168.1.22

;; Query time: 3 msec
;; SERVER: 192.168.1.26#53(192.168.1.26) (UDP)
;; WHEN: Mon Nov 03 17:06:14 CET 2025
;; MSG SIZE  rcvd: 100
```

(Consulta al NS del servidor Esclavo)

Prueba de Actualización SIN Incremento del Serial:

Esta prueba demuestra que el **número de Serial** es el único factor que BIND utiliza para determinar si una zona necesita ser actualizada.

Primero añadiremos un registro en el servidor **Maestro,** sin tocar el Serial del SOA en la siguiente ruta:

```
root@hamza:/home/hamza# sudo nano /etc/bind/db.hamza.net
```

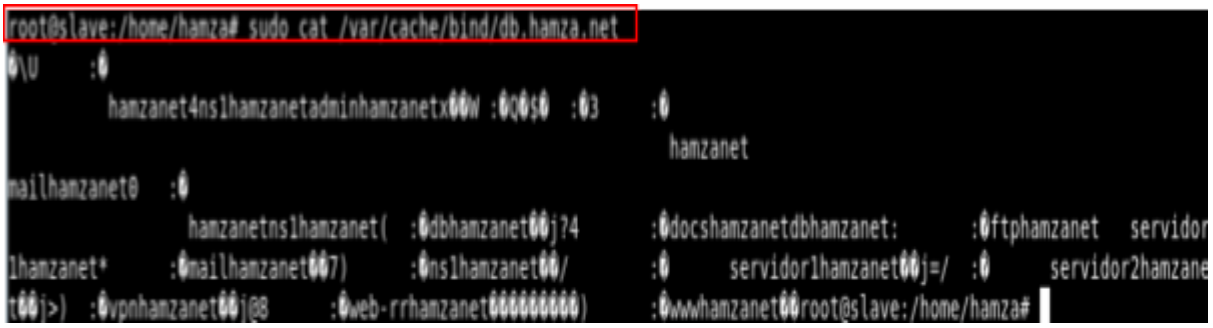
```
 GNU nano 8.4                    /etc/bind/db.hamza.net *

@       IN      NS      ns1.hamza.net.
ns1     IN      A       192.168.1.22

@       IN      MX 10   mail.hamza.net.
mail    IN      A       192.168.1.55

www     IN      A       192.168.1.23
servidor1 IN    A       192.168.106.61
servidor2 IN    A       192.168.106.62
db      IN      A       192.168.106.63
vpn     IN      A       192.168.106.64

test-sin-serial IN A 1.2.3.4
```

(Prueba de Actualización SIN Incremento del Serial)

Una vez realizada la configuración en el fichero para hacer la prueba, reiniciaremos nuestro servidor **Maestro y Esclavo** con los siguientes comandos:

```
sudo systemctl restart bind9
```

Utilizaremos el comando **sudo cat /var/cache/bind/db.hamza.net** para comprobar el contenido del fichero **Esclavo.** Para corroborar que se ha hecho de la manera correcta, no debería de aparecer ningún dato sobre la prueba-serial.



(Contenido prueba de fichero Esclavo)

Aplicando el comando expuesto arriba, el contenido no es muy legible, ya que no es en texto plano. Para solucionar este problema, forzaremos el volcado de la base de datos.

Primero, ejecutaremos el siguiente comando en la terminal del Servidor Esclavo. Este comando ordena al servicio **named,** que escriba su base de datos interna en un archivo de texto plano.

```
root@slave:/home/hamza# sudo rndc dumpdb -zones
```

Con el siguiente comando mostraremos el contenido del volcado hecho en el anterior paso:

```
root@slave:/home/hamza# sudo cat /var/cache/bind/named_dump.db
```

Una vez hecho el volcado, podemos observar que no aparece ningún dato sobre la prueba-serial.

```
; Zone dump of 'hamza.net/IN'
;
hamza.net.                              604800 IN SOA     ns1.hamza.net. admin.hamza.net. 2025110103 604800 86400
2419200 604800
hamza.net.                              604800 IN NS      ns1.hamza.net.
hamza.net.                              604800 IN MX      10 mail.hamza.net.
db.hamza.net.                           604800 IN A       192.168.106.63
docs.hamza.net.                         604800 IN CNAME   db.hamza.net.
ftp.hamza.net.                          604800 IN CNAME   servidor1.hamza.net.
mail.hamza.net.                         604800 IN A       192.168.1.55
ns1.hamza.net.                          604800 IN A       192.168.1.22
servidor1.hamza.net.                    604800 IN A       192.168.106.61
servidor2.hamza.net.                    604800 IN A       192.168.106.62
vpn.hamza.net.                          604800 IN A       192.168.106.64
web-rr.hamza.net.                       604800 IN A       192.168.1.201
web-rr.hamza.net.                       604800 IN A       192.168.1.202
web-rr.hamza.net.                       604800 IN A       192.168.1.203
www.hamza.net.                          604800 IN A       192.168.1.23
;
; Start view  bind
```

(Volcado de datos en la prueba sin serial)

Incrementa en el maestro el campo serial y reinicia de nuevo. Comprueba si ya aparece el nuevo registro en el secundario.

Prueba de actualización con incremento del Serial:

En el Servidor Maestro, editaremos el fichero de zona **/etc/bind/db.hamza.net** incrementando el número de serial en una unidad.

(Serial original, sin modificación)

Serial editado y aumentado en una unidad:

(Serial editado con una unidad más)

Una vez editado el fichero, reiniciaremos los servicios tanto del Maestro, como del Esclavo utilizando el siguiente comando. Esto activará la notificación (NOTIFY) hacia el Esclavo, y el Esclavo iniciará la transferencia al detectar el Serial mayor.

```
root@hamza:/home/hamza# sudo systemctl restart bind9
```

Ya reiniciado los servidores, comprobaremos el nuevo registro en el **servidor Esclavo,** pudiendo ver el nuevo registro**.**

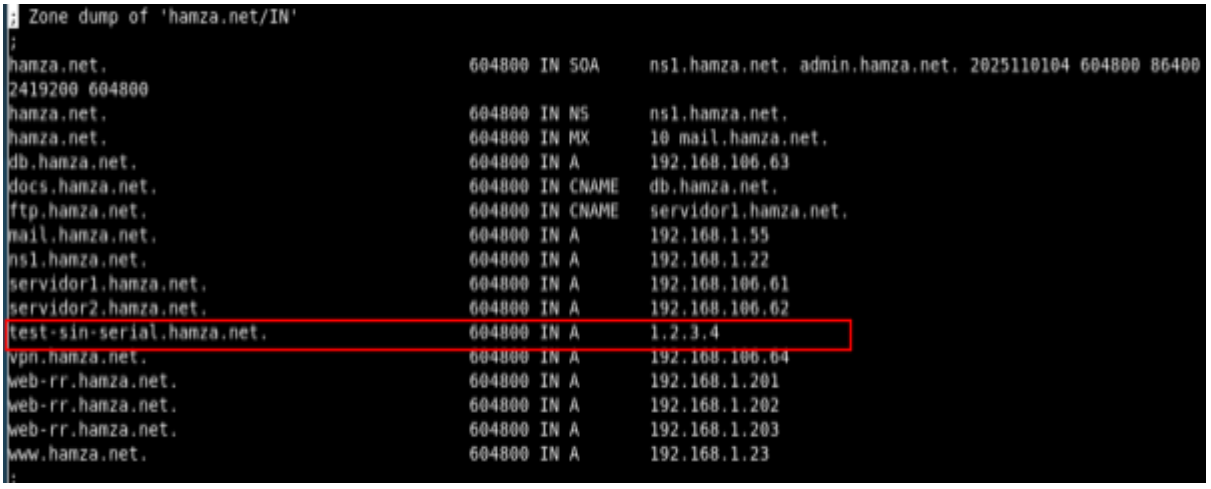
Primero volcaremos la base de datos actualizada con el siguiente comando:

```
root@slave:/home/hamza# sudo rndc dumpdb -zones
```

Hecho ya el volcado, pondremos el siguiente comando para visualizar los datos:

```
root@slave:/home/hamza# sudo cat /var/cache/bind/named_dump.db
```

Como podemos observar en la siguiente imagen, el registro sí aparece en el servidor secundario. Esto demuestra que el servidor esclavo inicia la transferencia de zona (**IXFR**) solo cuando el número de Serial del SOA en el servidor maestro es mayor que el suyo, validando el mecanismo de control de versiones de DNS.



(Prueba de actualización con incremento del Serial)

¿Cómo evitar que cualquier equipo le solicite al maestro una descarga del fichero de zona? Enlace. Realiza pruebas.

Para evitar que cualquier equipo solicite al servidor Maestro una descarga del fichero de zona, debemos utilizar la directiva de seguridad "**allow-transfer"** en la configuración de la zona dentro de **BIND**.

(Configuración del fichero con allow-transfer)

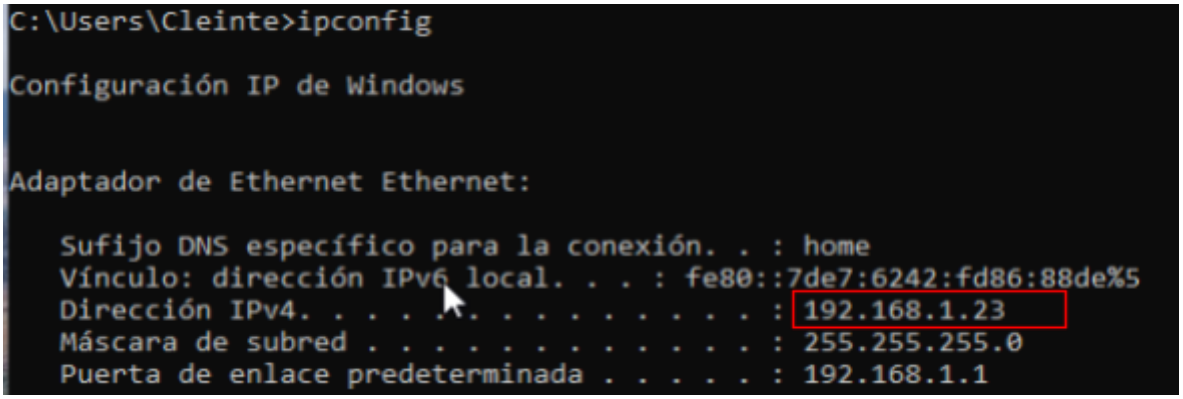
Después de modificar el archivo del Maestro, reiniciaremos BIND:

```
root@hamza:/home/hamza# sudo systemctl restart bind9
```

Para realizar pruebas, debemos intentar una transferencia de zona **desde una máquina no autorizada,** que este caso será una **máquina virtual de Windows.**

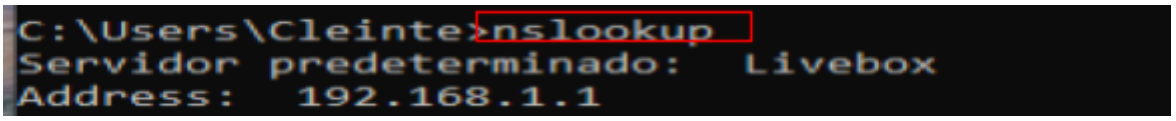
El objetivo es que rechace la solicitud de transferencia AXFR/IXFR proveniente de la IP **192.168.1.23** (máquina Windows), ya que esta IP no está en la lista de **allow-transfer.** Solo está el Servidor Esclavo, 192.168.1.26.

Haremos un **ipconfig** para dar a ver la ip de nuestra máquina Windows.



(IP máquina Windows no autorizada)

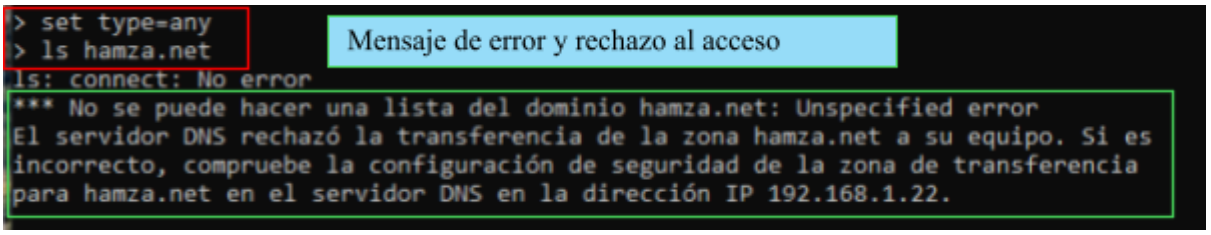
Para hacer la prueba, primero debemos iniciar la herramienta interactiva de consulta DNS de Windows **(nslookup).**



(Iniciación de herramienta nslookup)

Le dice a **nslookup** que dirija todas las consultas a tu Servidor Maestro (192.168.1.22).

Configuraremos el tipo de consulta para incluir todos los registros con el comando "**set type=any"** y terminar con forzando la transferencia de zona con el comando **"ls hamza.net"**



(Prueba de seguridad que la transferencia de zona es rechazada por el servidor Maestro)

Finalizando con el **mensaje de rechazo** tras el comando "**ls hamza.net."**

PARTE 2: REALIZACIÓN DE CONSULTAS ITERATIVAS Y RECURSIVAS CON HERRAMIENTAS PARA DEPURACIÓN

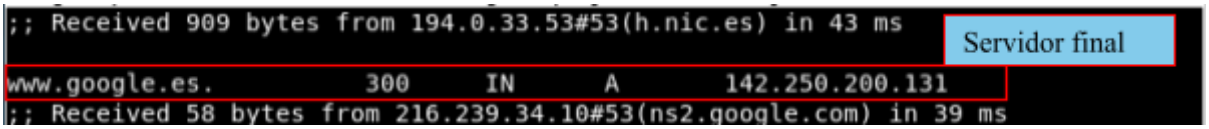
Realiza una consulta con el comando dig para consultar al servidor 8.8.8.8 la IP del dominio www.google.es. Activaremos la opción de traza para que nos dé información de los servidores encontrados en el proceso.

- Consulta Recursiva con Traza: El objetivo es simular el proceso de resolución completo que realiza un servidor DNS, desde la raíz hasta el servidor autorizado final.

dig @8.8.8.8 www.google.es +trace
El comando le pide al servidor de Google (8.8.8.8) que resuelva www.google.es y muestre todos los pasos.

```
root@hamza:/home/hamza# dig @8.8.8.8 www.google.es +trace
```

¿Qué servidor es el que finalmente nos da la IP?
El servidor que nos da la IP final (registro A) es el servidor autoritativo para el dominio google.es. Al analizar la traza, este es el último servidor consultado en la jerarquía, generalmente con un nombre como dnsX.google.com. Este servidor es el único que contiene la información precisa de los registros del dominio."



(Servido final/servidor autoritario de Google)

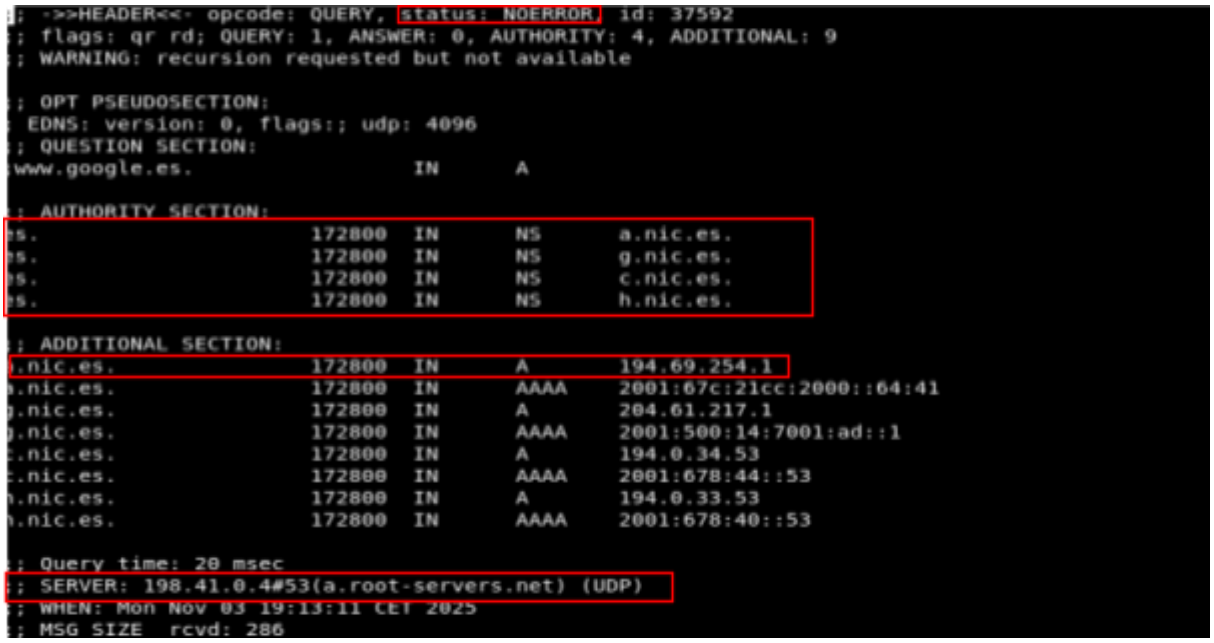
Realiza ahora paso a paso consultas iterativas partiendo de un servidor raíz hasta obtener la IP asociada al dominio. Empieza desde el servidor raíz. Por ejemplo: Con la información obtenida (elige un servidor para el dominio .es), continúa la secuencia de consultas iterativas hasta obtener la IP buscada.

Ahora, simularemos el proceso de **consultas iterativas** paso a paso para obtener la IP de un dominio, siguiendo la jerarquía de DNS.

El dominio objetivo va a ser www.google.es**.** Comenzaremos preguntando a uno de los servidores raíz con el siguiente comando:

```
root@hamza:/home/hamza# dig @a.root-servers.net www.google.es
```

El servidor raíz “**a.root-servers.net”** nos devolverá los servidores de nombres (**NS**) y sus direcciones IP para el dominio .es (**TLD**).



(Secuencia iterativa manual)

Anotaremos la dirección IP de uno de los servidores NS para **.es** que aparece en la sección **ADDITIONAL SECTION** (**194.69.254.1)**.

Una vez anotadas, preguntaremos al Servidor TLD con el siguiente comando, que le preguntará al servidor **.es** por el dominio www.google.es. **El servidor .es** remitirá a los servidores de nombres autoritativos para la zona google.es.

```
root@hamza:/home/hamza# dig @194.69.254.1 www.google.es
```

```
; <<>> DiG 9.20.15-1~deb13u1-Debian <<>> @194.69.254.1 www.google.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8879
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d2b2fe6adcd01ad3010000006908f364f2aa0a3fba2ac072 (good)
;; QUESTION SECTION:
;www.google.es.                 IN      A

;; AUTHORITY SECTION:
google.es.              86400   IN      NS      ns1.google.com.
google.es.              86400   IN      NS      ns3.google.com.
google.es.              86400   IN      NS      ns2.google.com.
google.es.              86400   IN      NS      ns4.google.com.

;; Query time: 8 msec
;; SERVER: 194.69.254.1#53(194.69.254.1) (UDP)
;; WHEN: Mon Nov 03 19:24:36 CET 2025
;; MSG SIZE  rcvd: 152
```

(Secuencia iterativa manual)

Dado que la última consulta no nos ha proporcionado dirección IP, debemos realizar una consulta adicional para obtener la **Ip** de alguna de los **NS**. Se hará entonces de **ns2.google.com**, como indica el siguiente comando:

```
root@hamza:/home/hamza# dig @8.8.8.8 ns2.google.com
```

Resuelto el nombre de uno de los servidores NS (ns2.google.com).

(Secuencia iterativa manual)

Después, anotaremos la dirección IP de uno de los **servidores NS** autoritativos de Google, que estarán en la sección **ADDITIONAL SECTION o AUTHORITY SECTION**. (216.239.34.10).

Por último, usaremos la última IP recogida del servidor autoritario (216.239.34.10) para consultar directamente al servidor de Google.

```
root@hamza:/home/hamza# dig @216.239.34.10  www.google.es
```

En los resultados, veremos en **ANSWER SECTION** con el registro **A** (IP de www.google.es), completando la secuencia iterativa manual.

(Secuencia iterativa manual)

PARTE FINAL

Escribe aquí la lista de ficheros de configuración utilizados en esta práctica con un breve resumen de la información que contienen.

Fichero	Descripción
/etc/hosts /etc/hostname	-Archivo utilizado para mapear direcciones IP locales a nombres de host. -Se modificó para identificar correctamente al servidor secundario en la red.
/etc/bind/named.conf.local	Es el archivo principal de configuración de zonas. Define el rol de cada servidor para la zona hamza.net. En el maestro, contiene la directiva de seguridad allow-transfer.

/etc/bind/db.hamza.net	Fichero de zona de resolución directa del **Servidor Maestro**. Contiene los registros autoritativos (`SOA`, `NS`, `A`, `MX`, `CNAME`) y el campo **Serial**, que se incrementa para forzar las transferencias al esclavo.
/var/cache/bind/db.hamza.net	**Fichero de zona de resolución directa del Servidor Esclavo.** Este archivo se genera automáticamente cuando el Servidor Esclavo realiza una transferencia de zona (AXFR o IXFR) desde el Servidor Maestro. Es una copia de la zona del Maestro. BIND lo actualiza automáticamente cada vez que el Serial del Maestro incrementa. Se almacena en el directorio de caché de BIND.

Escribe aquí la lista de ficheros de log, etc. utilizados en esta práctica con un breve resumen de la información que contienen.

Fichero	Descripción
/var/cache/bind/	**Directorio caché de BIND.** Almacena la **información dinámica** del servidor. Aquí el servidor esclavo guarda los ficheros de zona descargados y los ficheros **.jnl** utilizados para transferencias incrementales (IXFR).

	También almacena la caché de consultas recursivas.
/var/log/syslog	**Fichero de registro general del sistema.** Contiene los mensajes **log** generados por el sistema operativo, incluyendo información sobre el servicio BIND. Es útil para buscar errores al iniciar o reiniciar BIND, así como registros de seguridad relacionados con peticiones de transferencia.

Escribe aquí la lista de órdenes relacionadas con el DNS utilizadas en esta práctica con un breve resumen de lo que hacen.

Orden	Descripción
named-checkconf	Verifica la sintaxis general de los archivos de configuración de BIND. Es esencial para asegurar que BIND pueda iniciarse.
dig	**Herramienta para consultas DNS**. Se utiliza para diagnosticar la resolución, obtener tipos de registros específicos (SOA, NS) y realizar **trazas jerárquicas** (+trace y consultas iterativas manuales).
nslookup	**Herramienta de consulta DNS**. Se usa para probar la resolución de nombres, verificar la IP de un servidor DNS específico y en Windows, para intentar la transferencia de zona.
systemctl restart bind9	**Reinicia el servicio BIND**. Esta orden es necesaria después de cualquier

	modificación en los archivos de configuración para que BIND cargue los cambios.
named-checkzone	**Verifica la sintaxis de un fichero de zona específico** antes de cargarlo. Asegura que los registros estén correctamente formateados.
journalctl -u bind9	Muestra el **registro detallado** del servicio BIND. Es fundamental para el diagnóstico, ya que indica por qué el servicio falló al iniciar o por qué fue rechazada una transferencia de zona.

RESUMEN

Esta práctica ha sido muy completa porque pasamos de un solo servidor **DNS** a montar una infraestructura básica con alta disponibilidad usando un **Servidor Maestro** (**ns1.hamza.net) y un Esclavo (slave.hamza.net).** Configuramos el Esclavo como **type slave** y el **Maestro** con **“allow-transfer”** y al reiniciar, el fichero de zona se descargó automáticamente.

También me llamó mucho la atención la seguridad, al usar “**allow-transfer**” para que ningún otro equipo pudiera robar el fichero de zona. En general, la práctica sirvió para entender que un DNS no es solo un mapa de IPs, sino un sistema jerárquico y muy sensible a la configuración de redes y firewalls.

PROBLEMAS SURGIDOS DURANTE LA PRÁCTICA

Contenido Ilegible del Fichero de Zona Descargado:

Problema:El fichero de zona descargado por el esclavo (/var/cache/bind/db.hamza.net) aparecía codificado en binario al usar cat.

Para la documentación, se utilizó el comando **sudo rndc dumpdb -zones**. Esto forzó a BIND a volcar la base de datos a un fichero de texto plano legible, confirmando que la transferencia AXFR fue exitosa.