Francisco Javier López Calderón

Práctica 6: Sincronizar servidores DNS maestro y esclavo

Partiendo de la práctica anterior, configurar la sincronización entre el servidor DNS maestro y esclavo con las siguientes características:

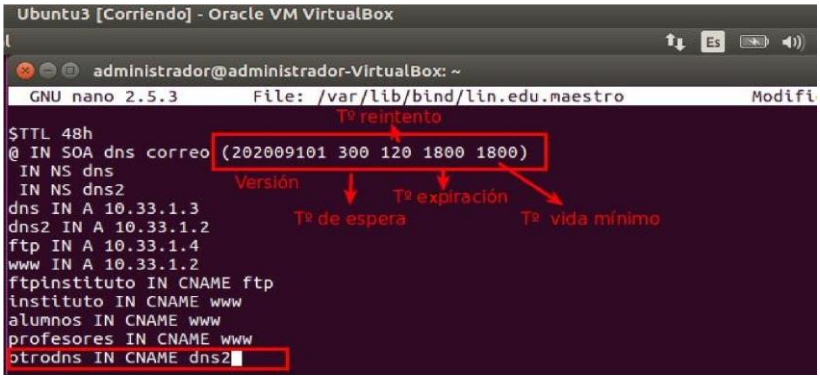
- La versión tendrá el formato año_mes_dia_versión (aaammddvv). P.e. 2020100301.

- Se debe obligar al esclavo a esperar 5 minutos para realizar el refresco, 2 minutos de frecuencia de reintentos, 30 minutos de tiempo de espiración y 30 minutos de tiempo de vida mínimo.

Nota: Ten en cuenta que para su resolución deberás utilizar el fichero de definición de zona con los registros de recursos más abreviados posible.

Deberás comprobar que:
- al añadir un nuevo registro de recursos automáticamente se actualiza el servidor esclavo.
- cuando no hay conexión con el maestro se desecha la información por parte del esclavo a los 30 minutos de forma automática (Deja de resolver, pero conserva el fichero que se le transfirió).
- si se vuelve a tener contacto con el maestro, pasados 5 minutos volverá a activarse la resolución del esclavo de forma automática.

1º) Con ambos servidores en marcha, editamos el fichero de definición de zona del maestro e introducimos los cambios necesarios para la sincronización que nos piden, así como un nuevo nombre de dominio que es un alias al dns2 que ya teníamos:



- El primer parámetro que aparece entre paréntesis en la línea SOA es el **número de serie o versión**, que se utiliza para que los esclavos se enteren de que ha habido cambios en el fichero de definición de zona maestro. Debemos aumentarlo en una unidad cada vez que modifiquemos el contenido del fichero. El servidor esclavo leerá este valor y, si es mayor que el que tiene almacenado, procederá a la actualización de su información de la zona (transferencia de zona), de forma inmediata o no.

- El segundo parámetro que aparece entre paréntesis en la línea SOA es el **refresh** o periodo de refresco. Indica la frecuencia en segundos con la que el esclavo consulta al maestro para ver si existe una actualización de la zona, en nuestro caso 5 minutos. Este parámetro solo se aplicará si la directiva **notify** *(que es una de las opciones del fichero named.conf.options) toma el valor 0*.

- El tercer parámetro (**retry**) significa que, si el esclavo no puede contactar con el maestro por fallo del servidor o de la red, se volverá a intentar más tarde (concretamente el número de segundo indicado en este parámetro)
- El parámetro **Expire** es el tiempo que los esclavos mantienen información sobre los maestros si no hay conexión.
- El último parámetro (**minimum**) es el tiempo de vida en caché.

Cuándo se realiza la transferencia de zona

Cada vez que hagamos algún cambio en el fichero de definición de zona maestro (añadir un nombre, eliminarlo o modificarlo) y modifiquemos su número de serie, debemos reiniciar el servidor bind9 del maestro. Esto puede provocar el refresco inmediato de los esclavos, o no.

La directiva NOTIFY, que se configura en el fichero /etc/bind/named.conf.local indica cuándo se produce la transferencia de zona:

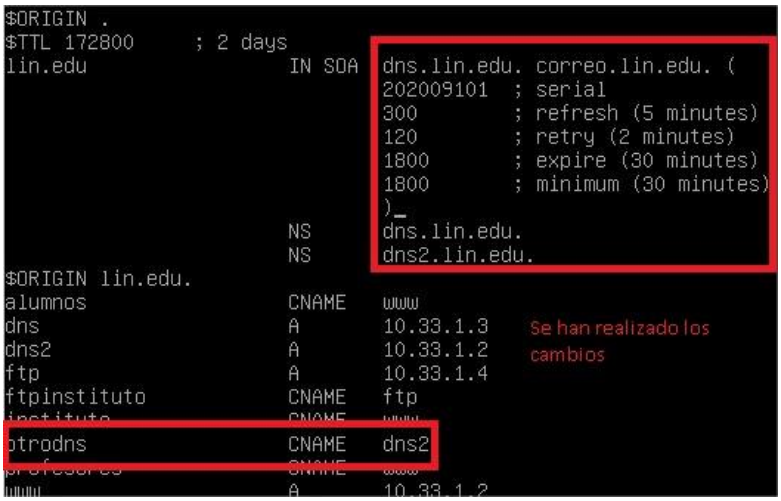
- Si notify es YES (valor por defecto) se actualiza el esclavo en cuanto se reinicia el maestro, sin hacer caso a los tiempos configurados en el apartado anterior. Si hay varios esclavos para un dominio, todos se refrescarán cuando se reinicie el mestro.

- Si notify es NO, los esclavos **NO** se actualizan cuando se reinicia el maestro, sino cada 5 minutos (se aplica el valor valor refresh). Esto quiere decir que, **cada 5 minutos**, los esclavos consultan el fichero de zona del maestro para ver si ha cambiado (si ha cambiado el número de versión). Si es así lo actualizan.

2º) Primero vamos a probar que si **notify** es **YES** (es el valor que toma por defecto, no hace falta modificar nada), el esclavo se actualiza en cuando se reinicia el maestro sin aplicar los tiempos de refresco que hemos configurado.
Recordar incrementar el número de versión **siempre** que se modifique el fichero de zona (ya lo hemos hecho en el apartado 1).

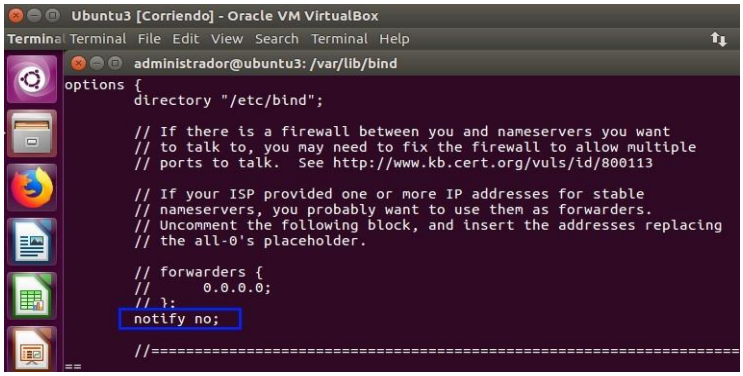
- Por lo tanto, reiniciamos el servidor maestro **ubuntu3** con el comando: sudo service bind9 restart

- Y editamos el fichero */var/lib/bind/lin.edu.esclavo de* ***Debian2*** para comprobar que se ha actualizado inmediatamente con los cambios introducidos en el apartado 1:



3º) Ahora vamos a poner la directiva **NOTIFY** con el valor **NO** para indicar que el esclavo no se refresque cuando se reinicie el maestro, sino cada cierto tiempo (en nuestro caso, 5 minutos, como hemos configurado). Para ello, editamos el fichero **/etc/bind/named.conf.options** del maestro Ubuntu3 y escribimos la directiva:

```
administrador@administrador-VirtualBox:~$ sudo nano /etc/bind/named.conf.options
```




```
//forwarders {
//;
//};
notify no;
```

A continuación, volvemos a modificar el fichero /var/lib/bind/lin.edu.maestro de Debian2 para añadir un nombre, sin olvidar incrementar el número de versión o serie:

```
administrador@administrador-VirtualBox:~$ sudo nano /var/lib/bind/lin.edu.maestro
```

```
$TTL 48h
@ IN SOA dns correo (20200902 300 120 1800 1800)
 IN NS dns
 IN NS dns2
dns IN A 10.33.1.3
dns2 IN A 10.33.1.2
ftp IN A 10.33.1.4
www IN A 10.33.1.2
ftpinstituto IN CNAME ftp
instituto IN CNAME www
alumnos IN CNAME www
profesores IN CNAME www
otrodns IN CNAME dns2
profesores2 IN CNAME www
```

```
$TTL 48h
@ IN SOA dns correo (202009102 300 120 1800 1800)
 IN NS dns
 IN NS dns2
dns IN A 10.33.1.3
dns2 IN A 10.33.1.2
ftp IN A 10.33.1.4
www IN A 10.33.1.2
ftpinstituto IN CNAME ftp
instituto IN CNAME www
alumnos IN CNAME www
profesores IN CNAME www
otrodns IN CNAME dns2
profesores2 IN CNAME www
```

Reiniciamos el servidor maestro Ubuntu3 y accedemos a la carpeta /var/lib/bind de Debian 2 para ver si el fichero del esclavo ya se ha actualizado. Lo más probable es que no sea así, puesto que no se actualiza inmediatamente, sino cada 5 minutos. Esperamos un rato y finalmente comprobamos que se ha actualizado:

Sin esperar los 5 minutos

```
$ORIGIN .
$TTL 172800     ; 2 days
lin.edu                 IN SOA  dns.lin.edu. correo.lin.edu. (
                                202009101  ; serial
                                300        ; refresh (5 minutes)
                                120        ; retry (2 minutes)
                                1800       ; expire (30 minutes)
                                1800       ; minimum (30 minutes)
                                )
                        NS      dns.lin.edu.
                        NS      dns2.lin.edu.
$ORIGIN lin.edu.
alumnos                 CNAME   www
dns                     A       10.33.1.3
dns2                    A       10.33.1.2
ftp                     A       10.33.1.4
ftpinstituto            CNAME   ftp
instituto               CNAME   www
otrodns                 CNAME   dns2
profesores              CNAME   www
www                     A       10.33.1.2
```

Se actualiza automáticamente tras 5 minutos

```
$ORIGIN .
$TTL 172800     ; 2 days
lin.edu                 IN SOA  dns.lin.edu. correo.lin.edu. (
                                202009102  ; serial
                                300        ; refresh (5 minutes)
                                120        ; retry (2 minutes)
                                1800       ; expire (30 minutes)
                                1800       ; minimum (30 minutes)
                                )
                        NS      dns.lin.edu.
                        NS      dns2.lin.edu.
$ORIGIN lin.edu.
alumnos                 CNAME   www
dns                     A       10.33.1.3
dns2                    A       10.33.1.2
ftp                     A       10.33.1.4
ftpinstituto            CNAME   ftp
instituto               CNAME   www
otrodns                 CNAME   dns2
profesores              CNAME   www
profesores2             CNAME   www
www                     A       10.33.1.2
```