PRÁCTICAS SERVIDORES DNS

Índice

1. INTRODUCCIÓN

Una vez instalado el servidor, como un rol más en nuestro servidor, podemos empezar a probar distintas configuraciones, a añandir RR y a realizar consultas a nuestro nuevo servicio para comprobar que las respuestas sean las esperadas.
Para probar nuestra práctica podemos asignar a un cliente nuestro, la IP de nuestro servidor en la red virtual que va a administrar (red interna), o la incluso podemos hacer que el DNS de nuestro servidor sea él mismo.
En principio, y dado que finalmente serán unos clientes los que utilicen nuestro servidor tanto para navegar como para obtener DHCP o para resolver sus consutlas DNS, **optamos por la opción de usar un cliente** (bien sea con el servidor DHCP instalado y configurado en el tema anterior o mediante una configuración estática del cliente).
Sería recomendable que cambiaras el nombre de tu equipo en Windows 2016 para que tenga un nombre mas legible por ejemplo *srvW2016Tunombre*

Una práctica interesante en cada SO, una vez hayamos instalado el servicio DNS sería hacer una consulta contra el servidor que acabamos de instalar para comprobar como la primera vez tarda bastante más que la segunda en resolver lo mismo. Por ejemplo con una llamada a nslookup con este formato

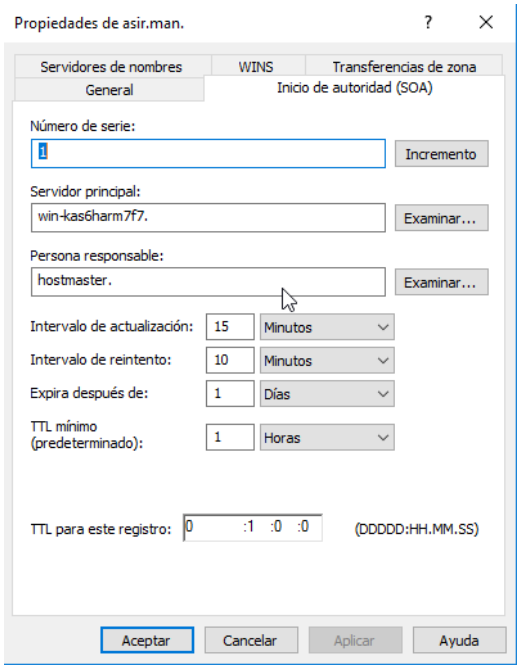
NSLOOKUP NombreDominio IP_SERVIDOR_DNS

¿Por que crees que se produce esto? Por qué los resultados de consultas del servidor se guardan en caché para acelerar las consultas futuras.

2. **WINDOWS SERVER**

A) Servidor Primario

- Debemos **BUSCAR** la configuración correcta para decirle a nuestro servidor que únicamente atienda las peticiones dentro de nuestra red privada virtual.
- Actuará como maestro y tendrá por tanto autoridad sobre el la zona directa vuestro_nombre.asir.com.
- Debe crearse la zona inversa asociada
- Acceder a las propiedades de la zona directa. En la ventana SOA vemos muchas cosas ¿Sabes que representan?



<u>Las características del servidor serán:</u>

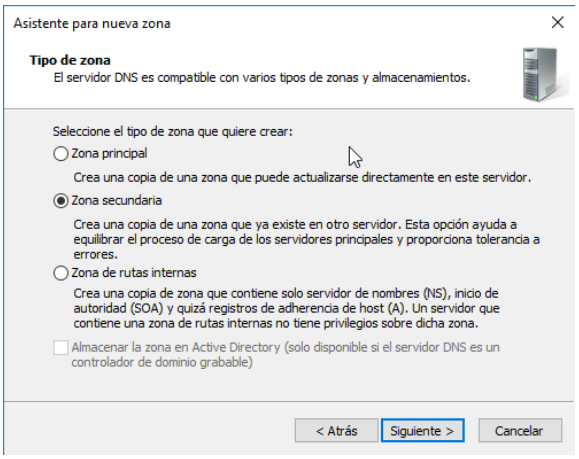
1. No permite actualizaciones automáticas
2. El servidor DNS maestro del dominio **srvW20Tunombre**(es decir el equipo donde está instalado el srv dns)
3. Incluir otra IP en vuestra red privada para que sea posteriormente un servidor autorizado en esta zona que estais creando ¿Donde crees que tendrías que hacerlo?
4. Registros de recursos que incluirá:
   A. Crear cuatro equipos (direcciones ip V4)
   B. Crear un alias para cada uno de los equipos anteriores
   C. Teneis los siguientes servicios en vuestro dominio. *Todos ellos balanceados con 3 servidores,* y funcionando en los puertos por defecto
      1. Servidor correo
      2. Servidor web
      3. Servidor LDAP

B) Servidor Secundario

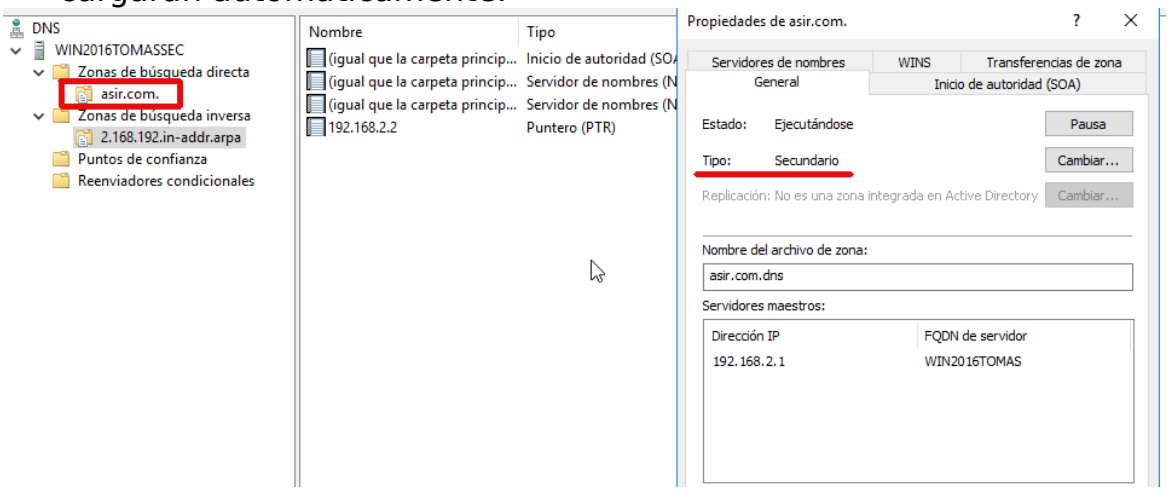
Vamos a intentar ejecutar 2 máquinas de Windows Server (+-3 GB cada una) para configurar un servidor ESCLAVO del que acabamos de crear en el punto anterior. Podéis encontrar multitud de manuales en la web. Aqui teneis un ejemplo que, aunque antiguo os puede ayudar bastante.

Antes de iniciar la configuración de DNS, comprobad bien la configuración de las tarjetas virtuales, tanto a nivel de Vbox, como la configuración IP que les habéis proporcionado. Comprobad además si algún firewall os impide el acceso a la otra máquina. Un simple PING para comprobar que se ven será suficiente.
En resumen, los pasos a realizar son:

1. Configurar el servidor maestro (Punto anterior).
2. Instalar el servicio DNS en un segundo servidor. Podemos clonar la plantilla que no tenia nada de Win2012|16 o clonar el servidor primario y eliminar DHCP, caso que lo tuviera. En este segundo caso elminiaríamos todas las zonas, ya que son las que hemos creado en el apdo. A.
3. Añadimos un *RR de tipo A* que apunte a nuestro servidor secundario.
4. Creamos **tanto en la zona directa como inversa del servidor maestro**, dentro de la pestaña **Servidores de nombres** las entradas para el servidor secundario, podemos buscarlo por nombre, ya que en el punto anterior lo hemos añadido como host (A).
5. Creación de la zona en el secundario. **TANTO LA DE BÚSQUEDA DIRECTA COMO LA DE BÚSQUEDA INVERSA**



6. En cuanto ambas zonas estén apuntando a su servidor maestro. Se cargarán automáticamente.



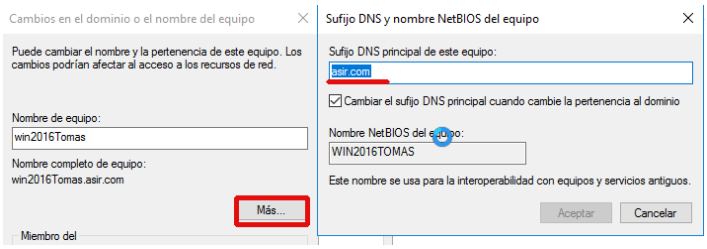
7. Accede a la pestaña SOA en el servidor secundario para modificar algunos valores. ¿Que es lo que ocurre?

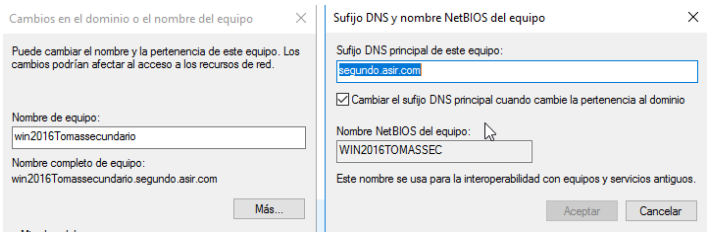
8. Realiza una modificación en el servidor primario y actualiza el secunadrio. ¿Que ocurre con el campo **serie**?

C) Delegación de zona

Como última actividad en cuanto a Windows Server y DNS Server, vamos a configurar el dominio vuestro_nombre.asir.com. para que delegue algún subdominio en otro servidor. Podemos guiarnos por lo que indica el siguiente tutorial. Hay que tener algunos aspectos importantes para que el proceso no falle:

1. En la ventana de modificación del nombre del equipo hay que incluir correctamente el SUFIJO (dominio) de cada equipo

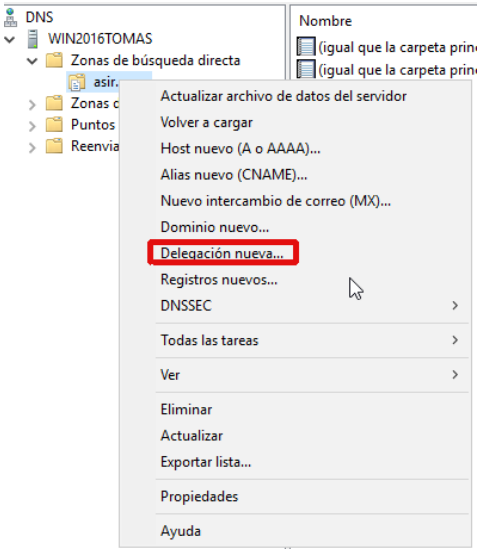


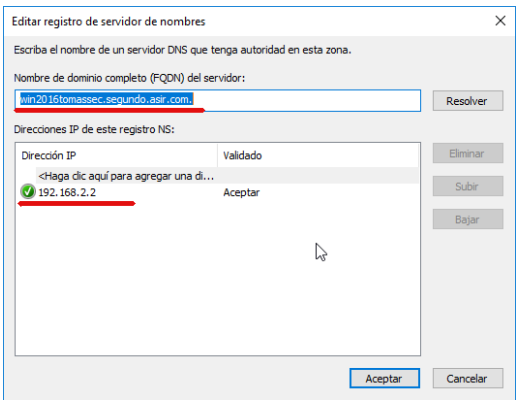


En el servidor principal

En el equipo en que se delega

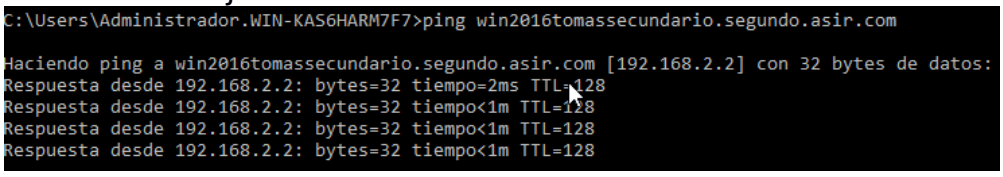
2. Creo las dos zonas como primarias en cada servidor.
3. En el servidor principal (en mi caso asir.com), realizo la delegación.



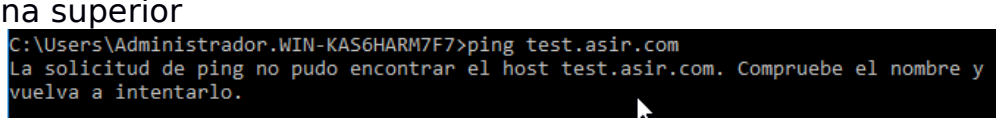


4. Debo indicar tanto el nombre como la IP ya que hasta que no esté finalizada la delegación WIN2016TOMAS (asir.com) no puede resolver WIN2016TOMASSEC (segundo.asir.com)

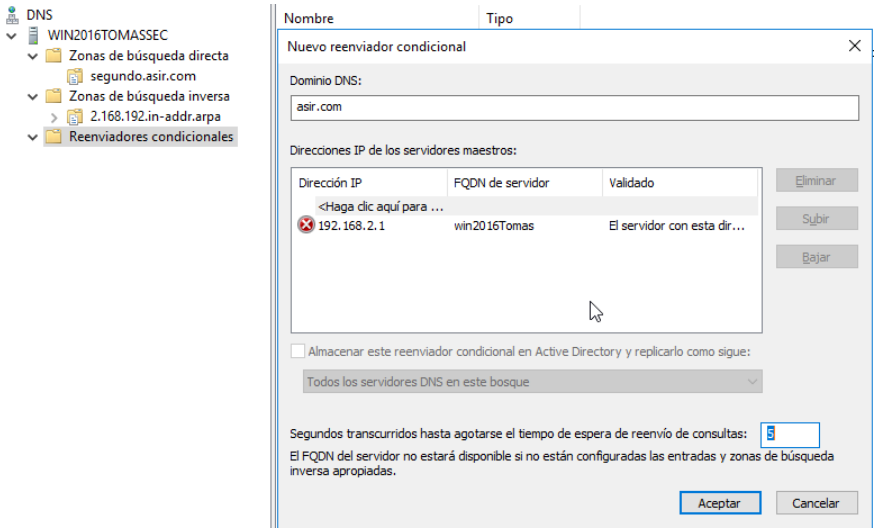
5. En esta situación, desde el DNS 'padre' puede resolver solicitudes sobre la zona 'hija'



Sin embargo desde el hijo no resuelve las solicitudes DNS sobre la zona superior



6. Si queremos que el servidor 'hijo' pueda resolver solicitudes DNS sobre la zona 'padre' debemos crear un reenviador condicional para esa zona.



De esta manera el servidor hijo también resuelve consultas sobre la zona padre.

<u>Para acabar, averigua en que ubicación están los ficheros de zona en windows, y si estos son parecidos a lo que esperabas.</u>

3. **UBUNTU SERVER (BIND)**

En esta sección vamos a utilizar intensamente el siguiente material, el cual nos va a permitir acercarnos a la herramienta BIND, la cual se utiliza en los sistemas debian para administrar el servicio DNS.

Inicialmente trabajaremos sin interfaz gráfica, aunque en la parte final de la práctica con Ubuntu, probaremos a realizar alguna tarea con la herramienta Webmin, que hemos instalado previamente.
Recordar hacer copias de seguridad de los ficheros existentes antes de comenzar las prácticas.

A) Servidor Primario

Realizaremos inicialmente una configuración de un servidor primario (master). Con las siguientes configuraciones **globales** (las incluimos, siguiendo la estructura de bind, en el fichero *named.conf.options*). Nuestro servidor tendrá las siguientes características:

1. Se permiten consultas recursivas, por lo tanto, el servidor aceptará consultas y él se encargará de conseguir las respuestas; al final se las entregará a los solicitantes.
2. Se permitirá las consultas recursivas solo a los equipos de las redes a las que está conectado el servidor.
3. NO muestra información sobre la versión de Bind.
4. El directorio para resolver las rutas relativas será /var/cache/bind.
5. El servidor escucha por el puerto por defecto de DNS, únicamente en su tarjeta local.
6. Las transferencias de zonas se prohibirán a todos los host a nivel global, y será desde cada zona, desde donde se permitarán a los equipos que interese.

Para conseguir estas configuraciónes, el fichero named.conf.options quedaría de la siguiente manera:

```
# cat /etc/bind/named.conf.options
options {
   directory "/var/cache/bind";
   version "No disponible";
   forwarders {8.8.8.8};
   listen-on port 53 { 192.168.200.254; }; #IP tarj. LOCAL del servidor
   recursion yes;
   allow-recursion { localnets; };
   allow-transfer { none; };
};
```

Vamos a configuar un servidor maestro, y por lo tanto, autoritario, para el dominio **asir.com**
(el fichero de zona será */var/cache/bind/db.master.asir.com*), incluyendo su zona inversa(fichero */var/cache/bind/db.master.192.168.2*). Por lo que en el fichero *named.conf.local* incluiriamos:

```
# cat /etc/bind/named.conf.local
zone "asir.com" in {
  type master;
  file "db.master.asir.com";
};

zone "200.168.192.IN-ADDR.ARPA" in {
  type master;
  file "db.master.192.168.200";
};
```

Observamos que no atendemos peticiones de transferencia, ya lo trataremos en los siguientes apartados.
Una vez tenemos las configuraciones generales de la zona, tanto directa como inversa, ya podemos comenzar a completar los dos ficheros de zona.
Las características del servidor serán:

1. No permite actualizaciones automáticas
2. El servidor DNS maestro del dominio **UBSRV20TOMAS**(es decir el equipo donde está instalado el srv dns). Para cambiar el nombre de tu equipo puedes seguir el siguiente tutorial.
3. Dos ejemplos sencillos de ficheros de zona, tanto directa como inversa, serían

Zona directa

```
; BIND reverse data file for empty rfc1918 zone
;
; FICHERO PARA LA ZONA ASIR.COM
;
$TTL    86400
$ORIGIN asir.com.

@ IN SOA ubsrv20tomas.asir.com. root.asir.com. (
                1               ; Serial
                604800          ; Refresh
                86400           ; Retry
                2419200                 ; Expire
                86400 ); Negative Cache TTL
                 ;
        IN      NS      ubsrv20tomas
ubsrv20tomas IN     A       192.168.200.254
www     IN      A       192.168.200.5
mail    IN      A       192.168.200.6
web     IN      CNAME www
@       IN      MX      10      mail
```

Zona inversa

```
; BIND reverse data file for empty rfc1918 zone
;
; FICHERO PARA LA ZONA INVERSA ASIR.COM EN LA
; RED 192.168.200.0/24
;
$TTL    86400
$ORIGIN 200.168.192.in-addr.arpa.

@ IN SOA ubsrv20tomas.asir.com. root.asir.com. (
                1               ; Serial
                604800          ; Refresh
                86400           ; Retry
                2419200         ; Expire
                86400 ); Negative Cache TTL
                ;
        IN      NS      ubsrv20tomas.asir.com.

254     IN      PTR     ubsrv20tomas.asir.com.
5       IN      PTR     www
6       IN      PTR     mail
```

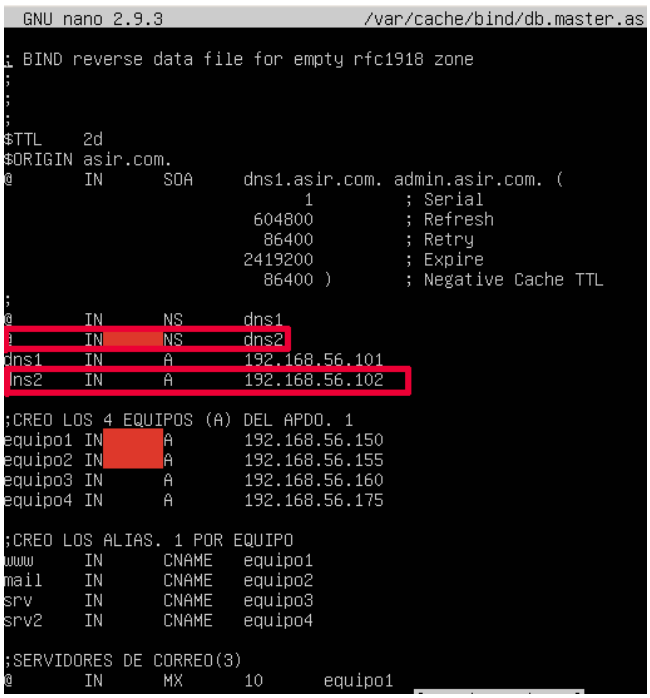
Usándolos como orientación, en nuestro caso no tenemos varios NS, ya que todavía no hablamos de servidores secundarios, crear los ficheros de zona para una zona que incluirá los siguientes Registros de Recursos.

A) Crear cuatro equipos (direcciones ip V4), y sus correspondencias en la zona inversa.
B) Crear un alias para cada uno de los equipos anteriores

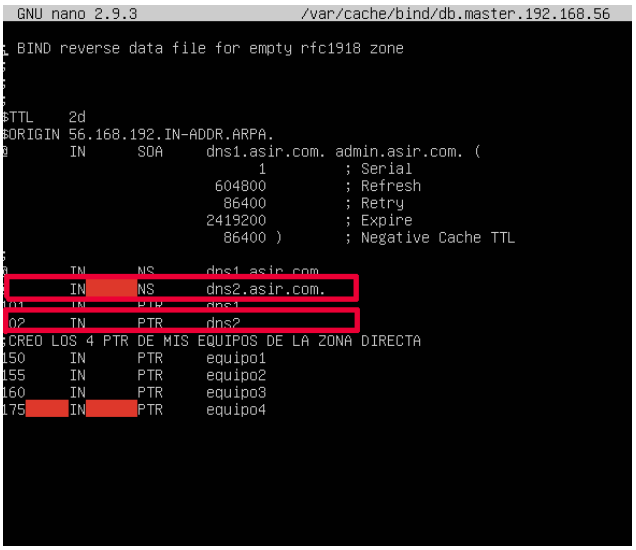
C) Tenéis los siguientes servicios en vuestro dominio. *Todos ellos balanceados con 3 servidores,* y funcionando en los puertos por defecto
   1. Servidor correo
   2. Servidor web
   3. Servidor LDAP

B) Servidor Secundario

En este ejercicio vamos a repetir el escenario de la práctica para Windows. Vamos a ejecutar 2 máquinas de Ubuntu Server (a diferencia de Windows, con 2 GB para cada una funcionarán razonablemente bien y el host no se bloqueará).
En el apartado anterior no hemos considerado en ningún momento la posibilidad de incluir servidores secundarios, **de ahí que únicamente haya una entrada NS en el fichero de zona directa**.
Para añadir el nuevo servidor DNS secundario, deberíamos añadir algo como lo siguiente en nuestro fichero de zona en el servidor ppal.
1.- ZONA DIRECTA

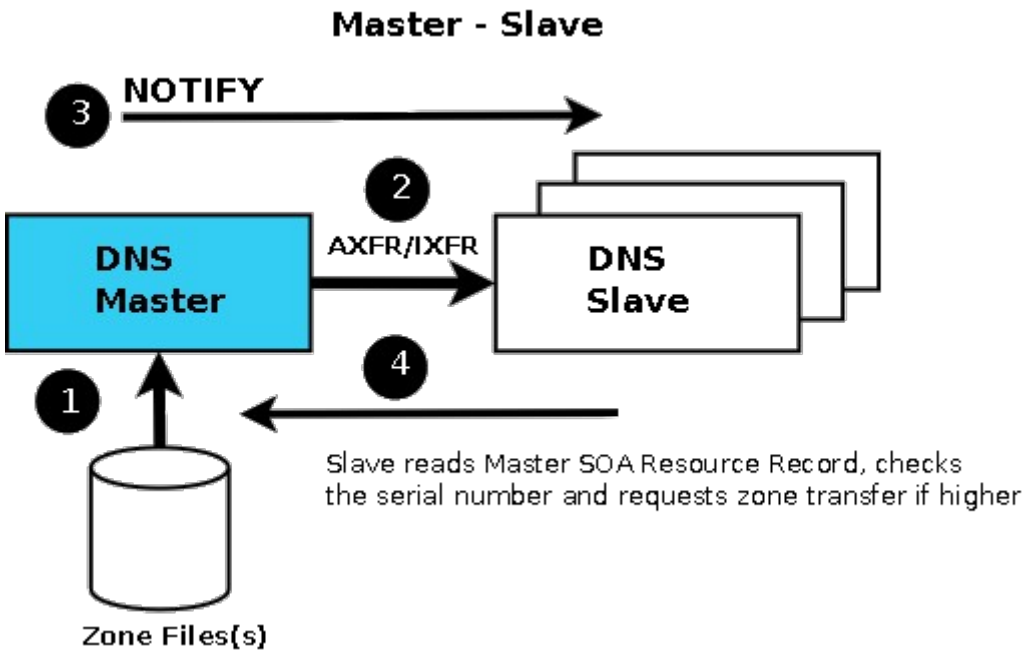


Zona directa



Zona inversa

Recordamos que el servidor secundario únicamente recibe el fichero de zona del maestro en un proceso denominado TRANSFERENCIA DE ZONA.



¿AXFR/IXFR?

Las Transferencias de zona dns, a veces llamadas AXFR por el tipo de solicitud, es un tipo de transacción de DNS. Es uno de varios mecanismos disponibles para administradores para replicar bases de datos DNS a través de un conjunto de servidores DNS. La transferencia puede hacerse de dos formas: completa (AXFR) o incremental (IXFRX). Se producirá una transferencia de zona durante cualquiera de los siguientes escenarios:

1. Al iniciar el servicio DNS en el servidor DNS secundario.
2. Cuando caduca el tiempo de actualización.
3. Cuando se guardan los cambios en el archivo de zona principal y hay una notificación lista.

Con respecto a la configuración global de BIND en el servidor secundario, mantendremos el mismo comportamiento global que para el servidor maestro, desactivando los mensajes NOTIFY del esclavo, ya que solo el servidor maestro emite dichos mensajes:

1. Directorio para las rutas relativas: /var/cache/bind.
2. No se dará información sobre la versión de BIND.
3. El servidor escuchará SOLO por la interfaz local, por el puerto 53.
4. El servidor funcionará como caché DNS para las redes a las que está conectado.
5. Se prohibirán las transferencias de zona.
6. Se prohibirán los mensajes NOTIFY.

```
# cat /etc/bind/named.conf.options
options {
   directory "/var/cache/bind";
   version "No disponible";
    listen-on port 53 { 192.168.2.2 };   #la IP de mi tarjeta LOCAL
es la 192.168.2.2
   recursion yes;
   allow-recursion { localnets; };
```

```
    allow-transfer { none; };
    notify no;
};
```

Un aspecto importante a tener en cuenta en el Servidor Maestro es permitir las transferencias de zona. En el punto anterior no las hemos tenido en cuenta y las hemos prohibido a nivel global. Tendríamos que autorizarlas en cada zona de la siguiente manera:

```
zone "asir.com" in {
    type master;
    file "db.master.asir.com";
                    allow-transfer
{ 192.168.2.2; };
};
```

```
zone              "2.168.192.IN-
ADDR.ARPA" in {
    type master;
    file "db.master.192.168.2";
                    allow-transfer
{ 192.168.2.2; };
};
```

<u>Una buena práctica sería realizar esto como se ha hecho en la web en que nos estamos apoyando. ¿Que te parece esa estrategia?</u>

Una vez hemos dicho en el servidor primario a quien podemos transferir las zonas, quedaría por definir estas zonas en el servidor secundario, creándolas como secundarias e informando de quién es el servidor primario:

```
zone "asir.com" in {
    type slave;
    file "db.slave.asir.com";
    masters { 192.168.2.1; };
                    allow-notify
{ 192.168.2.1;  };
};
```

```
Zone  "2.168.192.IN-ADDR.ARPA"
in {
    type slave;
    file "db.slave.192.168.2";
    masters { 192.168.2.1; };
    allow-notify { 192.168.2.1;  };
};
```

Con esto ya debería funcionar el proceso de TRANSFERENCIA DE ZONA, hay que recordar incluir como NS en el fichero de zona al servidor que acabamos de añadir. Si todo ha ido bien en el servidor secundario deberíamos ver algo como:

```
administrador@ubuntu_server_18_04:~$ sudo service bind9 restart
administrador@ubuntu_server_18_04:~$ sudo service bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: en
   Active: active (running) since Mon 2018-10-22 09:01:04 UTC; 1s ago
     Docs: man:named(8)
  Process: 5258 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 5262 (named)
    Tasks: 4 (limit: 2315)
   CGroup: /system.slice/bind9.service
           └─5262 /usr/sbin/named -f -u bind

oct 22 09:01:04 ubuntu_server_18_04 named[5262]: zone 2.168.192.IN-ADDR.ARPA/IN:
oct 22 09:01:04 ubuntu_server_18_04 named[5262]: transfer of '2.168.192.IN-ADDR.
oct 22 09:01:04 ubuntu_server_18_04 named[5262]: zone 2.168.192.IN-ADDR.ARPA/IN:
oct 22 09:01:04 ubuntu_server_18_04 named[5262]: transfer of '2.168.192.IN-ADDR.
oct 22 09:01:04 ubuntu_server_18_04 named[5262]: transfer of '2.168.192.IN-ADDR.
oct 22 09:01:05 ubuntu_server_18_04 named[5262]: zone asir.com/IN: Transfer star
oct 22 09:01:05 ubuntu_server_18_04 named[5262]: transfer of 'asir.com/IN' from
oct 22 09:01:05 ubuntu_server_18_04 named[5262]: zone asir.com/IN: transferred s
oct 22 09:01:05 ubuntu_server_18_04 named[5262]: transfer of 'asir.com/IN' from
oct 22 09:01:05 ubuntu_server_18_04 named[5262]: transfer of 'asir.com/IN' from
```

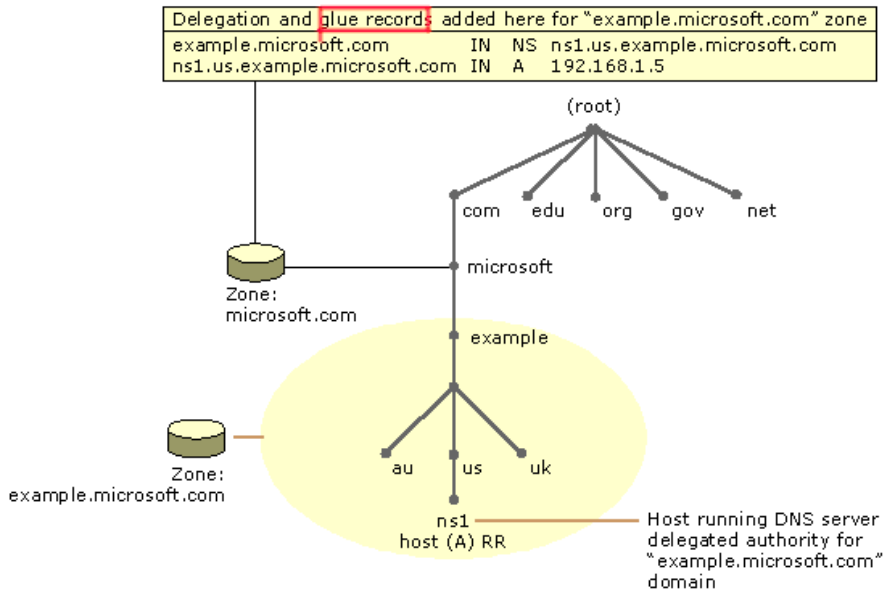
Mientras que en el servidor maestro deberíamos poder consultar el log con un comando como ***$cat /var/log/syslog | grep named,*** mostrando algo

```
Oct 22 09:01:04 srvub1804tomas named[4807]: client @0x7f00400b8ea0 192.168.2.2#37229 (2.168.192.IN-ADDR.ARPA): transfer of '2.168.192.IN-ADDR.
ARPA/IN': AXFR started (serial 2016040800)
Oct 22 09:01:04 srvub1804tomas named[4807]: client @0x7f00400b8ea0 192.168.2.2#37229 (2.168.192.IN-ADDR.ARPA): transfer of '2.168.192.IN-ADDR.
ARPA/IN': AXFR ended
Oct 22 09:01:05 srvub1804tomas named[4807]: client @0x7f00404d8a90 192.168.2.2#48917 (asir.com): transfer of 'asir.com/IN': AXFR started (seri
al 2016040800)
Oct 22 09:01:05 srvub1804tomas named[4807]: client @0x7f00404d8a90 192.168.2.2#48917 (asir.com): transfer of 'asir.com/IN': AXFR ended
```

como:

C) Delegación de zona

Como ya sabemos, el proceso de delegación de zona consiste en autorizar a otro servidor DNS la gestión de una zona hija, por parte del servidor principal de la zona que alberga a la 'sub-zona' que se delega. Este proceso es una de las bases de todo el protocolo DNS, y permite distribuir el Espacio de Nombres de Dominio.



La delegación se configura en el servidor 'padre', y obviamente, maestro, mediante la inclusión de dos lineas en el fichero de zona, y en la zona delegada obviamente debe declararse correctamente el servidor maestro. Para configurar la delegación de zona DNS, haga lo siguiente, teniendo como domino padre asir.com, con el que estamos trabajando en todos los supuestos prácticos.

Elija un nombre de dominio para la zona a delegar (por ejemplo, tomas.asir.com).

Agregue registros a la zona principal del dominio elegido para delegar y la dirección IP del servidor Master de esa zona. En mi ejemplo (atentos a los puntos finales ¡¡FQDN!!):

```
;AÑADIDO A MI FICHERO DE ZONA
; definiciones de subdominio
; fragmento de zona para tomas.asir.com

$ ORIGIN tomas.asir.com.
@ IN NS ns1.omas.asir.com.
ns1.omas.asir.com. IN A 192.168.2.2  ; glue-record
```

```
; ADVERTENCIA: $ORIGIN tomas.asir.com. afecta a todos los RRs posteriores hasta encontrar otro $ORIGIN o el EOF
; añadiendo $ORIGIN asir.com. Restablecemos al nombre de dominio base
```

Después de esto ya puede configurar su zona delegada como hemos aprendido en el apdo. A.

Open — db.master.asir.com — /var/cache/bind

```
$TTL 2d
$ORIGIN asir.com.

@         IN    SOA   srvub1804tomas.asir.com. hostmaster.asir.com. (
                      2016040801  ; se = serial number
                      12h         ; ref = refresh
                      15m         ; ret = refresh retry
                      3w          ; ex = expiry
                      2h          ; nx = nxdomain ttl
                      )
          IN    NS    srvub1804tomas
          IN    NS    ns2
          IN    NS    ns3

srvub1804tomas       IN    A        192.168.2.1
ns2       IN    A          192.168.2.2
ns3       IN    A          192.168.2.3
prof      IN    A          192.168.2.1
www       IN    A          192.168.2.1
ftp       IN    CNAME      www

$ORIGIN tomas.asir.com.
@       IN  NS  ns1sub
ns1sub  IN  A   192.168.2.2
```

El fichero de la zona delegada sería algo como:

```
$ORIGIN tomas.asir.com.

@         IN    SOA   ns1sub.tomas.asir.com. hostmaster.tomas.asir.com.
                      2016040800  ; se = serial number
                      12h         ; ref = refresh
                      15m         ; ret = refresh retry
                      3w          ; ex = expiry
                      2h          ; nx = nxdomain ttl
                      )
          IN    NS    ns1sub

ns1sub       IN    A         172.16.0.2
```

Con esto ya tendríamos una zona delegada pero hay que tener en cuenta una cosa.

¿Reenviadores condionales?

Se pueden definir reenviadores por dominio, lo que nos puede ayudar mucho en la delegación de zona. ¿Puedes ver el problema?

```
zone "asir.com" {
        type forward;
        forwarders {192.168.2.1;};
};
```