5. Servicios de red (I)

- Compartición de archivos en Linux: NFS
- Compartición de archivos Windows y entornos mixtos: Samba
- Servidores de nombres: DNS, WINS

- Práctica 6: Configuración de una intranet con servidor Windows. DNS. Samba

5.L NFS

- NFS (Network File System) sirve para que un sistema de ficheros que reside en un host remoto pueda montarse de forma local
- En el equipo servidor se debe indicar qué sistemas de archivos se exportan (puede ser un sistema completo o sólo una parte), a qué ordenadores se exportan y en qué condiciones (sólo lectura, lectura/escritura, etc.)
- En el equipo cliente se monta el sistema de ficheros remoto mediante la orden mount
- Un equipo puede ser servidor y cliente al mismo tiempo

5.L Configuración de un servidor NFS

- Un host puede indicarse mediante su nombre o su dirección IP
- Pueden usarse comodines, como *.example.com (los puntos no se incluyen en el comodín; one.example.com está incluido pero one.two.example.com no lo está)
- Las redes pueden expresarse como a.b.c.d/z (p.e. 192.168.0.0/24) o con su máscara de red a.b.c.d/netmask (192.168.100.8/255.255.255.0)

5.L Configuración de un servidor NFS

- Los servidores NFS pueden configurarse editando manualmente el archivo **/etc/exports** o mediante la utilidad **exportfs** (veremos solo el primer método).
- La sintaxis del fichero /etc/exports es:
  - Se ignoran las líneas en blanco
  - Los comentarios comienzan con #
  - Puede usarse el símbolo “\” para concatenar dos líneas
  - Las listas de hosts autorizados se sitúan después del sistema de archivos exportado y se separan con espacios
  - Las opciones de cada uno de los hosts se indican ente paréntesis después del nombre de cada host, sin dejar espacios:

    export host1(opciones1) host2(opciones2) host3(opciones3)

5.L Configuración de un servidor NFS

- Ejemplo:

  /exported/directory uno.example.com

- El formato del archivo /etc/exports es muy preciso; las siguientes dos líneas no tienen el mismo significado:

  /home bob.example.com(rw)

  /home bob.example.com (rw)

- En la primera, todos los usuarios de bob.example.com pueden acceder a /home con acceso de lectura y escritura. En la segunda, los usuarios de bob.example.com pueden acceder como lectura (acceso por defecto) y todos los usuarios del mundo pueden acceder como lectura/escritura

5.L Configuración de un servidor NFS

- Las opciones por defecto son:
  - **ro** (sólo lectura, los hosts remotos no pueden modificar el sistema de archivos exportado)
  - **sync** (el servidor no atiende peticiones nuevas hasta que las anteriores hayan sido escritas a disco – el recíproco es **async**)
  - **wdelay** (se retrasa la escritura a disco si se sospecha que hay una nueva solicitud de escritura de forma inminente – el recíproco es **no_wdelay**)
  - **root_squash** (los usuarios "root" de los hosts remotos no tienen privilegios de root en el sistema de archivos; el servidor NFS les asocia el ID **nfsnobody** a los recursos propiedad de root – el recíproco es **no_root_squash**. También puede usarse la opción **all_squash** para que todos los usuarios remotos se mapeen a nfsnobody, o indicar uid y gid

    export host(anonuid=uid,anongid=gid)

5.L Instalación e inicio de NFS

- Se instala el paquete nfs-utils: **yum install nfs-utils**
- Se inicia el servicio y se habilita automáticamente cuando se bota el servidor mediante

  systemctl enable --now nfs-server
- Se reinicia con

  systemctl restart nfs-server
- La versión más reciente de NFS es NFSv4. NFSv2 y NFSv3 requieren que esté corriendo el servicio **rpcbind**, para el cual deben abrirse los puertos correspondientes en el firewall
- Para que NFS solamente admita clientes v4 se añaden las siguientes líneas a la sección [nfsd] del archivo de configuración **/etc/nfs.conf**

  [nfsd]

  vers2=no

  vers3=no
- Desde el cliente, se monta con la orden mount:

  mount –t nfs a.b.c.d/nombre_share punto_de_montaje

5.L Firewall para NFS

- Si se instala NFSv4 solo es necesario abrir el puerto 2049/tcp

```
[root@localhost ~]# firewall-cmd --add-port=2049/tcp --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp1s0
  sources:
  services: ssh dhcpv6-client samba
  ports: 2049/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

5.L Verificación de la configuración NFS

```
[root@localhost ~]# netstat --listening --tcp --udp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:mountd          0.0.0.0:*               LISTEN
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:48825           0.0.0.0:*               LISTEN
tcp        0      0 localhost:smtp          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:36512           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:nfs             0.0.0.0:*               LISTEN
tcp6       0      0 [::]:32879              [::]:*                  LISTEN
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
tcp6       0      0 [::]:mountd             [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN
tcp6       0      0 localhost:smtp          [::]:*                  LISTEN
tcp6       0      0 [::]:nfs                [::]:*                  LISTEN
tcp6       0      0 [::]:41350              [::]:*                  LISTEN
udp        0      0 0.0.0.0:mountd          0.0.0.0:*
udp        0      0 localhost.locald:domain 0.0.0.0:*
udp        0      0 localhost.locald:domain 0.0.0.0:*
udp        0      0 0.0.0.0:bootps          0.0.0.0:*
udp        0      0 0.0.0.0:bootps          0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp        0      0 0.0.0.0:sunrpc          0.0.0.0:*
udp        0      0 0.0.0.0:925             0.0.0.0:*
udp        0      0 localhost:927           0.0.0.0:*
udp        0      0 0.0.0.0:41923           0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 0.0.0.0:nfs             0.0.0.0:*
udp        0      0 0.0.0.0:47235           0.0.0.0:*
udp        0      0 0.0.0.0:43213           0.0.0.0:*
udp6       0      0 [::]:48251              [::]:*
udp6       0      0 [::]:60893              [::]:*
udp6       0      0 [::]:mountd             [::]:*
udp6       0      0 [::]:sunrpc             [::]:*
udp6       0      0 [::]:925                [::]:*
udp6       0      0 [::]:nfs                [::]:*
[root@localhost ~]#
```

5.L Compartición de archivos con Windows: samba

- Windows comparte las impresoras y los archivos con protocolos basados en NetBIOS. Samba es un servicio Linux que permite a una máquina Linux ser cliente de un servidor Windows y también alojar recursos y compartirlos a una máquina Windows.

- El protocolo empleado entre los clientes y los servidores NetBIOS es el Server Message Block Protocol (SMB),

- Para correr NetBIOS se necesita un protocolo capaz de llevar datos NetBIOS sobre TCP/IP y una técnica para asociar direcciones NetBIOS a direcciones TCP/IP. Samba proporciona ambos servicios: el daemon **smbd** proporciona los servicios de compartición de archivos e impresoras y el daemon **nmbd** asocia nombres a direcciones IP. Adicionalmente, el daemon **winbindd** proporciona un interface para NSS (Name Service Switch) para usar Directorio Activo y poder autentificar a los usuarios del dominio

5.L Instalación e inicio de Samba

- Se instala el paquete nfs-utils: **yum install samba**

- La utilidad testparm verifica la configuración de Samba en /etc/samba/smb.conf

```
[root@localhost ~]# testparm
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Registered MSG_REQ_POOL_USAGE
Registered MSG_REQ_DMALLOC_MARK and LOG_CHANGED
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
        printcap name = cups
        security = USER
        workgroup = SAMBA
        idmap config * : backend = tdb
        cups options = raw


[homes]
        browseable = No
        comment = Home Directories
        inherit acls = Yes
        read only = No
        valid users = %S %D%w%S


[printers]
        browseable = No
        comment = All Printers
        create mask = 0600
        path = /var/tmp
        printable = Yes


[print$]
        comment = Printer Drivers
        create mask = 0664
        directory mask = 0775
        force group = @printadmin
        path = /var/lib/samba/drivers
        write list = @printadmin root
```

5.L Samba (opciones)

- la opción "security" tiene varias alternativas:
    - **share**: nivel más bajo. El usuario se autentifica sólo con una password.
    - **user**: cada usuario se autentifica con un nombre y una password. Dependiendo de las opciones indicadas en passdb, la password se indica de forma independiente a la password del sistema con el comando smbpasswd
    - **domain, ads**: similares a user (usuario, password) pero la autentificación se gestiona por una máquina externa o un dominio.

5.L Samba (opciones)

- Opciones para restringir el acceso a determinadas redes:
  - **host allow/deny**: lista de hosts y redes que pueden conectarse con el servidor
  - **interfaces**: lista de interfaces en que escucha el servidor

5.L Samba: sección [homes]

- **browseable**: si está a no, sólo los usuarios con user/pass correcto pueden ver los nombres de los archivos. El acceso al contenido del share está limitado por los permisos Linux
- **writable**: ficheros sólo lectura
- **valid users**: lista de usuarios que pueden acceder a este share
- **create mode**: permisos con que se crea un archivo desde samba en homes
- **directory mode:** permisos de creación de un directorio

5.L Samba: Compartir directorios

```
[pcdocs]
    comment = PC Documentation
    path = /usr/doc/pcdocs
    browseable = yes
    writable = no
    public = yes

[research]
    comment = Research Department Shared Directory
    path = /home/research
    browseable = no
    writable = yes
    create mode = 0750
    hosts allow = host1,host2,host3
```

- El nombre del recurso va entre corchetes
- Cada uno de los shares está definido por su path y sus opciones

5.L Instalación de un servidor autónomo

- Se edita el fichero /etc/samba/smb.conf y se indica **security=user**, el fichero de log y la sección con los ficheros compartidos (en este caso, **[ejemplo]**)

```
# See smb.conf.example for a more detailed config file or
# read the smb.conf manpage.
# Run 'testparm' to verify the config is correct after
# you modified it.

[global]
        workgroup = Servidor-Samba-Ejemplo
        netbios name = ServidorEjemplo
        security = user
        log file = /var/log/samba/%m.log
        log level = 1

        passdb backend = tdbsam

        printing = cups
        printcap name = cups
        load printers = yes
        cups options = raw

[ejemplo]
        path = /srv/samba/ejemplo
        read only = no

[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        browseable = No
        read only = No
        inherit acls = Yes

[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @printadmin root
        force group = @printadmin
        create mask = 0664
        directory mask = 0775
```

5.L Instalación de un servidor autónomo

- Se verifica la configuración con el comando testparm
- Se abren los puertos del firewall

  firewall-cmd --permanent --add-service=samba

  firewall-cmd –reload
- Se reinicia el servicio (o se indica que arranque al botar el servidor)

  systemctl restart smb (systemctl enable smb)

```
[root@localhost ~]# testparm
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Registered MSG_REQ_POOL_USAGE
Registered MSG_REQ_DMALLOC_MARK and LOG_CHANGED
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[ejemplo]"
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions
```

5.L Utilidad smbpasswd

- La utilidad **smbpasswd** maneja las cuentas de usuario y las contraseñas en la base de datos local de Samba. Las contraseñas Linux no se encriptan de la misma forma que las contraseñas Windows y por tanto se precisa añadir a la base de datos local a cada usuario que vaya a acceder a un recurso compartido y asignarle contraseña.
- Los usuarios samba deben estar creados como usuarios locales en el sistema
- Debe estar instalado el paquete **samba-common-tools**
- **smbpasswd** desde un usuario cambia su contraseña
- **smbpasswd –a** desde root permite crear usuarios nuevos

5.L Utilidad smbstatus

- La utilidad **smbstatus** muestra las conexiones al servidor samba y varias estadísticas
- En el ejemplo, el share llamado "ejemplo" está siendo accedido desde la máquina con IP 192.168.7.69

```
[root@localhost ~]# smbstatus

Samba version 4.9.1
PID     Username     Group        Machine                                   Protocol Version  Encryption           Signing
----------------------------------------------------------------------------------------------------------------------------------------
15005   root         root         192.168.7.69 (ipv4:192.168.7.69:45386)    SMB3_11           -                    partial(AES-128-CMAC)

Service      pid     Machine       Connected at                     Encryption   Signing
---------------------------------------------------------------------------------------------
ejemplo      15005   192.168.7.69  Mon Nov  4 12:31:58 2019 CET     -            -

No locked files
```

5. Nombres y direcciones

- Se puede asignar un nombre (hostname) a cualquier dispositivo que tenga una dirección IP. El sistema convertirá el hostname a una dirección antes de realizar la conexión. Hay dos formas comunes de organizar los nombres de un sistema de computadores:
    - Espacio de nombres plano: Un identificador con una única parte identifica a un host
    - Espacio de nombres jerárquico: Se subdivide la red en partes con nombre, llamadas dominios. Cada hostname debe ser único dentro de un dominio.
- Originalmente, tanto NetBIOS como TCP/IP usaban un espacio de nombres plano. En la actualidad, se usan espacios jerárquicos.

5. Fichero HOSTS y DNS

- El método original de resolución de un nombre en TCP/IP consiste en mantener una tabla que asocia nombres y direcciones.

- Inicialmente (antes de haber servidores DNS para resolver las direcciones) se empleaba un archivo para almacenar esa tabla (archivo “hosts”). Es un archivo de texto plano que puede editarse. El archivo hosts sigue teniendo algunos usos.

- Actualmente, para traducir nombres TCP/IP a direcciones se emplea un sistema de nomenclatura jerárquico y descentralizado, llamado Domain Name Server (DNS)

5. Ejemplo de fichero HOSTS

```
# Table of IP addresses and hostnames
 172.16.12.2     pooh.example.com pooh
 127.0.0.1       localhost
 172.16.12.1     thoth.example.com thoth www
 172.16.12.4     wotan.example.com wotan
 172.16.12.3     kerby.example.com kerby
 172.16.1.2      kiwi.example.com kiwi
 172.16.6.10     thor.sales.example.com thor.sales thor
```

- Cada entrada contiene una dirección IP separada por un espacio en blanco de una lista de hostnames asociados con esa dirección

- Los comentarios comienzan por #

5. Usos del fichero HOSTS

- Esta tabla ha sido reemplazada por DNS, pero aún se usa en algunas ocasiones.
    - Puede servir como backup de emergencia en caso de que el DNS esté caído
    - En Linux, los sitios que usan NIS emplean el fichero hosts como entrada para la base de datos de hosts. Aunque puede usarse NIS en conjunción con DNS, la mayoría de los sitios NIS crean tablas de hosts que tienen una entrada para cada host en la red local
    - Los sitios muy pequeños que no están conectados a Internet usan en ocasiones el fichero hosts por simplicidad
    - Pueden añadirse definiciones de hosts para solucionar problemas de seguridad

5.L Fichero LMHOSTS (Samba)

- El método original de resolución de un nombre en NetBIOS consiste, al igual que en TCP/IP, en mantener una tabla que asocia nombres y direcciones.

- Al igual que ocurre con el archivo "hosts", esta tabla puede almacenarse en un archivo llamado “LMHOSTS”

- Actualmente, la base de datos usada para traducir nombres NetBIOS a direcciones se llama Windows Internet Name Service (WINS)

5.L Ejemplos de fichero LMHOSTS (I)

```
172.16.6.16      anubis
172.16.6.10      thor
172.16.6.7       theodore
```

- El fichero LMHOSTS es similar al HOSTS, y adicionalmente soporta algunos comandos prefijados por el símbolo #:
  - PRE: hace que la entrada se carge en la cache y se mantenga allí (mejora la velocidad para nombres usados frecuentemente)
  - #DOM: domain: Identifica a un servidor windows que puede validar peticiones de acceso a la red
  - #INCLUDE file: Especifica un fichero remoto que se incorpora al LMHOSTS local. Si se encierra una lista de #INCLUDEs entre un par #BEGIN_ALTERNATE/#END_ALTERNATE el sistema trata de descargar los archivos en orden y se detiene en cuanto lo consigue

5.L Ejemplos de fichero LMHOSTS

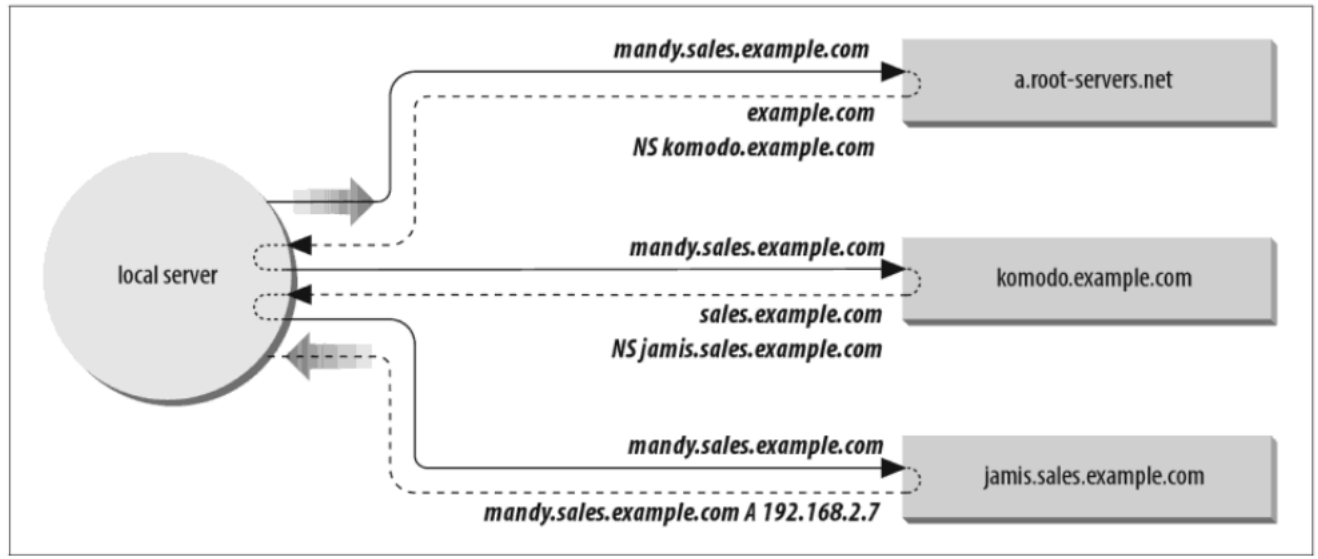
```
172.16.6.16      anubis      #PRE #DOM:ACCOUNTS
172.16.6.10      thor
172.16.6.7       theodore    #PRE
#BEGIN_ALTERNATE
#INCLUDE \\mandy\admin\lmhosts
#INCLUDE \\theodore\admin\lmhosts
#END_ALTERNATE
```

- Se cargan en la cache anubis y theodore
- Sin WINS, se necesita indicar qué ordenador es el controlador de dominio (anubis, y el dominio es ACCOUNTS)
- Se incluye \\mandy\admin\lmhosts y si no \\theodore\admin\lmhosts

5. Funcionamiento del DNS

- Es un sistema descentralizado, donde cada servidor almacena registros con información de algunos dominios y apunta a otros servidores para responder a las consultas de las que no haya información.
- Si un servidor DNS recibe una petición de información acerca de un host para el que no tiene datos, pasa esa petición a un *authoritative server,* que mantiene información acerca del dominio que sirve.
- Cuando el authoritative server contesta, el servidor local almacena (*caches*) la respuesta para usos futuros, de forma que si se vuelve a realizar la misma petición, el servidor contesta directamente
- Dentro de la estructura DNS, un subdominio es accesible cuando se inscriben los ordenadores que sirven el nuevo dominio en el dominio que está sobre él. El registro en la base de datos DNS que apunta a los servidores de nombres de un dominio es el registro “name server” (NS)

5. Consultas no recursivas DNS



- Un servidor local tiene una petición para resolver mandy.sales.example.com. El servidor no tiene información acerca del dominio example.com, por lo que consulta a un servidor raíz (a.root-servers.net). El servidor raíz contesta con un registro NS que apunta a komodo.example.com. El servidor local consulta a komodo, que a su vez devuelve un puntero a jamis.sales.examples.com como servidor para sales.example.com. El servidor local consulta a jamis que finalmente devuelve la dirección IP. El servidor local cachea el registro A (Address) y cada uno de los registros NS, de forma que la siguiente vez que el servidor reciba una consulta de mandy.sales.example.com la responde directamente, y para cualquier otra consulta que involucre a example.com irá directamente a komodo sin consultar a un root server.

5. DNS resolver y server

- El software DNS está dividido conceptualmente en dos componentes: el resolucionador (*resolver*) y el servidor de nombres.
- Todos los computadores resuelven hostnames, pero no todos actúan como servidores de nombres. Un ordenador que no tiene un servidor de nombres local se llama sistema "*resolver-only*"
- De acuerdo con su configuración, los servidores de nombres pueden ser
    - **Primario** (o *master*): servidor del que deriva toda la información de un dominio. Son autoritarios (*authoritative*): tienen información completa y la respuesta siempre es correcta. Hay un servidor primario por dominio
    - **Secundario**: transfiere la base de datos del dominio desde el servidor primario. Una base de datos para un dominio particular se llama *zone file*; copiar este fichero a un servidor secundario se llama zone file transfer. Un servidor secundario o esclavo (*slave*) asegura que tiene información correcta transfiriendo periódicamante el fichero de zona del dominio. Son autoritarios para su dominio.
    - **Solo cache** (*caching only*): consiguen las respuestas a las consultas consultando a otros servidores, y almacenan las respuestas. Son *nonauthoritative*.
- En Linux, la implementación de DNS es el *Berkeley Internet Name Domain* (BIND). El resolver es código enlazado con cualquier programa que necesite resolver direcciones, mientras que el servidor es un proceso llamado named.

5.L Configuración DNS Linux

- En Unix, DNS se implementa mediante el software Berkeley Internet Name Domain (BIND).
- La parte cliente de BIND es el resolver. Genera las consultas para la información de nombres de dominio y se las envía al servidor.
- La parte servidor es un daemon llamado **named**
- La configuración de BIND tiene 3 partes:
  - Configurar el resolver
  - Configurar el servidor de nombres
  - Construir los ficheros de base de datos del servidor de nombres (ficheros de zona)

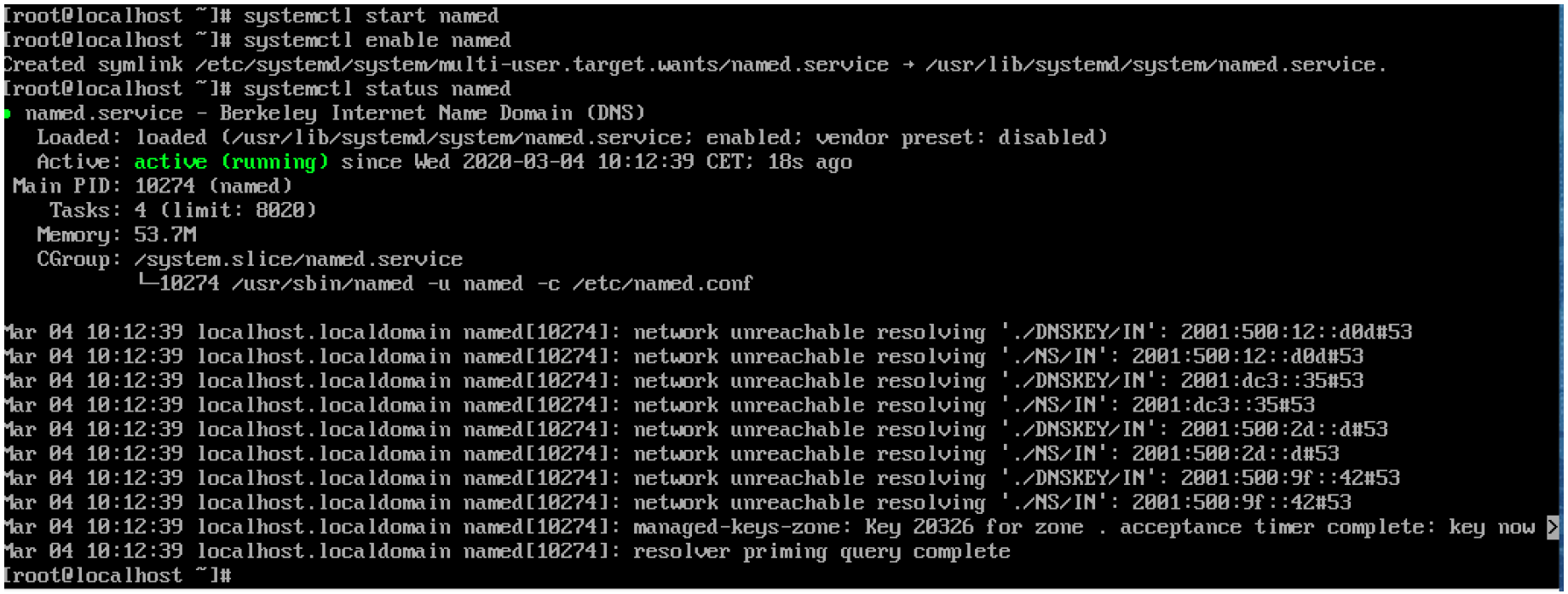
5.L Instalación BIND Linux

```
[root@localhost ~]# dnf install bind
Last metadata expiration check: 0:15:19 ago on Wed 04 Mar 2020 09:54:37 AM CET.
Dependencies resolved.
================================================================================
 Package                Arch              Version                 Repository  Size
================================================================================
Installing:
 bind                   x86_64            32:9.11.4-26.P2.el8     AppStream  2.1 M
Installing dependencies:
 bind-libs              x86_64            32:9.11.4-26.P2.el8     AppStream  170 k
 bind-libs-lite         x86_64            32:9.11.4-26.P2.el8     AppStream  1.1 M
 bind-license           noarch            32:9.11.4-26.P2.el8     AppStream   99 k

Transaction Summary
================================================================================
Install  4 Packages

Total download size: 3.6 M
Installed size: 8.7 M
Is this ok [y/N]: y
```

5.L Instalación BIND Linux



5.L DNS Linux

- Los niveles de servicio que pueden ser definidos en la configuración de BIND son 4: resolver-only, caching-only, master y slave.
- “resolver” es el código que pregunta a los servidores de nombres por la información del dominio. En UNIX, se implementa mediante una librería (no hay un daemon asociado)
- Las otras tres configuraciones son:
  - **Master**: fuente autoritaria para una zona. Su configuración requiere crear un fichero de zona para kas resoluciones directa e inversa, y los ficheros conf, root hints y loopback.
  - **Slave**: sólo requiere crear los ficheros boot, cache y loopback (los de zona se descargan del master)
  - **Caching-only**: ficheros boot y cache, generalmente también loopback.

5.L DNS Linux: resolver

- La parte resolver se configura mediante el archivo /etc/resolv.conf
- Las entradas son:
  - nameserver: dirección IP del servidor de nombres. Si no existe esta entrada se usa la dirección local. Para especificar la dirección local explícitamente se usa 0.0.0.0. Esta entrada no aparecerá en configuración "sólo resolver" (resolver-only)
  - domain: nombre de dominio por defecto, se añade a cualquier nombre que no contenga un punto. La variable LOCALDOMAIN se superpone a esta definición
  - search: Series de dominios buscados cuando el nombre de host no contiene un punto (se prueban en orden)

```
[root@localhost ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search Home
nameserver 212.231.6.7
nameserver 46.6.113.34
nameserver fe80::1%enp0s3
[root@localhost ~]#
```

5.L Configuración de named

- Ficheros de configuración:
  - parámetros generales: named.conf
  - root hints (puede llamarse named.ca db.cache, named.root, root.ca)
  - localhost: named.local (para resolver la dirección loopback)
  - resolución directa (o “fichero de zona”, p.e. midominio.com.hosts)
  - resolución inversa (p.e. 172.16.rev, para conocer el nombre de una IP)

5.L named.conf - caching only

- Estudiaremos diferentes configuraciones. La más sencilla es el servidor “caching-only”
- La primera opción indica el directorio por defecto de named
- Las instrucciones “zona” aparecen en todas las configuraciones. La primera define el fichero hints que se usa para localizar los servidores raíz en el arranque.
- La segunda hace que este servidor sea el master para su propia dirección loopback, y que la información de ese dominio (loopback) está en el fichero named.local
- El dominio loopback es un dominio “in-addr.arpa”, que asocia la dirección 127.0.0.1 al nombre localhost.

```
options {
        directory "/var/named";
};

// a caching only name server config

zone "." {
        type hint;
        file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};
```

5.L named.conf - caching only

```
options {
        directory "/var/named";
        forwarders { 172.16.12.1; 172.16.1.2; };
};
```

- Si se le añade la opción “forwarders” todas las peticiones que no se puedan resolver se redirigen a servidores específicos
- La opción “forward-only” hace que en ningún caso se intente resolver un nombre localmente

5.L named.conf - master

```
options {
        directory "/var/named";
};

// a master name server configuration

zone "." {
        type hint;
        file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};

zone "wrotethebook.com" {
        type master;
        file "wrotethebook.com.hosts";
};

zone "16.172.in-addr.arpa" {
        type master;
        file "172.16.rev";
};
```

- La tercera orden zone declara que éste es el servidor master para el dominio “wrotethebook.com”, y que los datos de ese dominio están en el archivo “wrotebook.com.hosts”

- La cuarta orden indica cuál es el archivo que asocia las direcciones 172.16.0.0 a nombres de hosts (servidor maestro para el dominio inverso 16.172.in-addr.arpa) - el archivo es 172.16.rev

5.L named.conf - esclavo

```
options {
        directory "/var/named";
};
// a slave server configuration
zone "." {
        type hint;
        file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};
zone "wrotethebook.com" {
        type slave;
        file "wrotethebook.hosts";
        masters { 172.16.12.1; };
};
zone "16.172.in-addr.arpa" {
        type slave;
        file "172.16.rev";
        masters { 172.16.12.1; };
};
```

- En las tercera zona se indica que se descarguen los datos de 172.16.12.1 y se almacenen en wrotebook.hosts. Si el archivo existe, sólo se descarga si su contenido es antiguo.

- La cuarta zona hace lo mismo con el archivo 172.16.rev

5.L Registros estándar de recursos

- SOA: Start of authority. Marca el comienzo de una zona y define parámetros que afectan a esa zona
- NS: Nameserver. Identifica un servidor de nombres del dominio
- A: Address. Convierte el nombre de host a una dirección
- PTR: Pointer. Convierte una dirección a un nombre de host
- MX: Mail Exchange. Servidor intermedio para reparto de correo
- CNAME: Canonical Name. Define un alias
- TXT: Text. Cadenas arbitrarias de texto

5.L Formato de un RR DNS

- [name] [ttl] IN type data
  - name: nombre de un objeto del dominio al que se refiere el recurso. Puede ser un host o el dominio completo. Es relativo al dominio actual salvo que termine en un punto. Si está en blanco, se aplica al objeto de dominio al que se haya referenciado por última vez.
  - ttl: time to live. En segundos, tiempo en que esta definición se guarda en el cache. La directiva $TTL afecta a toda la zona, suele dejarse en blanco este campo.
  - IN: el registro es un recurso Internet DNS
  - type: tipo de registro de recurso, ver transparencia anterior
  - data: información específica de ese tipo (p.e. dirección IP en un registro tipo A)

5.L Directivas de zona

- $TTL time-to-live
- $ORIGIN nombre que se usa para completar el dominio, por defecto el nombre indicado en la instrucción zone
- $INCLUDE lee un fichero externo
- $GENERATE crea una serie de registros, ver ejemplo en la transparencia siguiente

5.L Ejemplo

```
$ORIGIN 20.16.172.in-addr.arpa.
$GENERATE 1-4 $ CNAME $.1to4
```

- crea la serie de registros

```
1 CNAME 1.1to4
2 CNAME 2.1to4
3 CNAME 3.1to4
4 CNAME 4.1to4
```

- que equivalen a

```
1.20.16.172.in-addr.arpa. CNAME 1.1to4.20.16.172.in-addr.arpa.
2.20.16.172.in-addr.arpa. CNAME 2.1to4.20.16.172.in-addr.arpa.
3.20.16.172.in-addr.arpa. CNAME 3.1to4.20.16.172.in-addr.arpa.
4.20.16.172.in-addr.arpa. CNAME 4.1to4.20.16.172.in-addr.arpa.
```

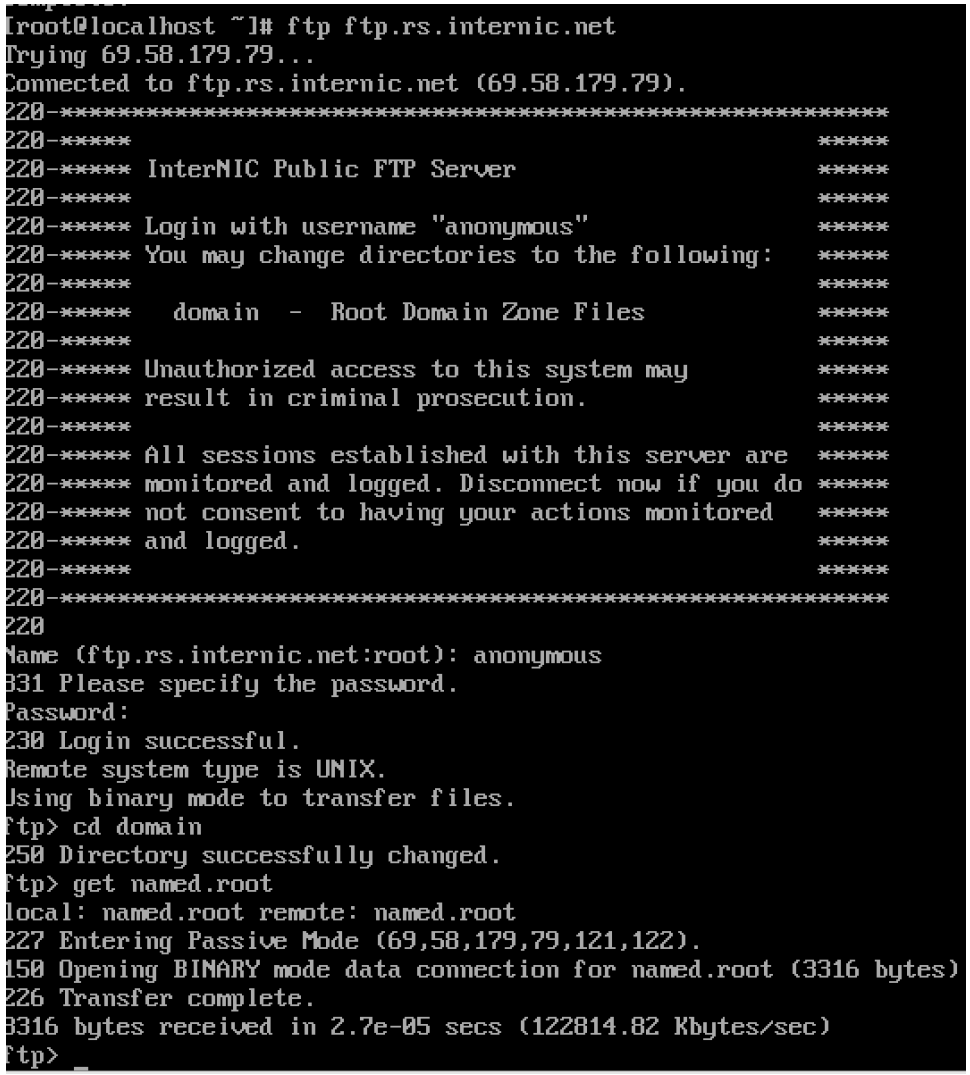
5.L El fichero de cache de inicialización

- La instrucción zone en named.conf tiene como tipo hints. Se usa cuando arranca named.

- El fichero named.root (/var/named/named.ca en RHEL 8) contiene registros NS para los servidores raíz y registros A con sus direcciones.

```
[root@localhost ~]# cat named.root
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     February 20, 2020
;       related version of root zone:     2020022000
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     199.9.14.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
E.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:a8::e
;
```

5.L El fichero de cache de inicialización



- Se puede obtener por ftp, bajándose el fichero domain/named.root de ftp.rs.internic.net con ftp anónimo

5.L El fichero named.local

- Se usa para convertir la dirección 127.0.0.1 en el nombre localhost; es el fichero de zona para el dominio inverso 0.0.127.in-addr.arpa

```
$TTL    86400
@       IN  SOA     crab.wrotethebook.com. alana.crab.wrotethebook.com. (
                    1               ; serial
                    360000          ; refresh every 100 hours
                    3600            ; retry after 1 hour
                    3600000         ; expire after 1000 hours
                    3600            ; negative cache is 1 hour
                    )
        IN  NS      crab.wrotethebook.com.
0       IN  PTR     loopback.
1       IN  PTR     localhost.
```

5.L named.local

```
$TTL    86400
@       IN  SOA     crab.wrotethebook.com. alana.crab.wrotethebook.com. (
                    1               ; serial
                    360000          ; refresh every 100 hours
                    3600            ; retry after 1 hour
                    3600000         ; expire after 1000 hours
                    3600            ; negative cache is 1 hour
                    )
        IN  NS      crab.wrotethebook.com.
0       IN  PTR     loopback.
1       IN  PTR     localhost.
```

- El registro SOA y el registro NS identifican la zona y el servidor de nombres de la zona
- El primer registro PTR asocia la dirección 127.0.0.0 con el nombre loopback
- El segundo registro PTR asocia la dirección 1 de la red 127.0.0.0 con el nombre localhost

5.L named.local

- Los ficheros named.conf, named.ca y named.local son los únicos requeridos para configurar servidores sólo-caché y servidores esclavos.

- Los restantes archivos sólo se usan en los servidores maestros

5.L El fichero de búsqueda inversa

```
$TTL 86400
;
;        Address to hostname mappings.
;
@       IN      SOA     crab.wrotethebook.com. jan.crab.wrotethebook.com. (
                                2001061401   ;   Serial
                                21600        ;   Refresh
                                1800         ;   Retry
                                604800       ;   Expire
                                900 )        ;   Negative cache TTL
                IN      NS      crab.wrotethebook.com.
                IN      NS      ora.wrotethebook.com.
                IN      NS      bigserver.isp.com.
1.12            IN      PTR     crab.wrotethebook.com.
2.12            IN      PTR     rodent.wrotethebook.com.
3.12            IN      PTR     horseshoe.wrotethebook.com.
4.12            IN      PTR     jerboas.wrotethebook.com.
2.1             IN      PTR     ora.wrotethebook.com.
6               IN      NS      linuxuser.articles.wrotethebook.com.
                IN      NS      horseshoe.wrotethebook.com.
```

- En este ejemplo se muestra el fichero 172.16.rev, para el dominio 16.172.in-addr.arpa

5.L El fichero de búsqueda directa

```
$TTL 86400
;       Addresses and other host information.
@       IN      SOA     crab.wrotethebook.com. jan.crab.wrotethebook.com. (
                                2001061401   ;   Serial
                                21600        ;   Refresh
                                1800         ;   Retry
                                604800       ;   Expire
                                900 )        ;   Negative cache TTL
;       Define the name servers and the mail servers
                IN      NS      crab.wrotethebook.com.
                IN      NS      ora.wrotethebook.com.
                IN      NS      bigserver.isp.com.
                IN      MX      10 crab.wrotethebook.com.
                IN      MX      20 horseshoe.wrotethebook.com.
;       Define localhost
localhost       IN      A       127.0.0.1
;       Define the hosts in this zone
crab            IN      A       172.16.12.1
loghost         IN      CNAME   crab.wrotethebook.com.
rodent          IN      A       172.16.12.2
                IN      MX      5 crab.wrotethebook.com.
mouse           IN      CNAME   rodent.wrotethebook.com.
horseshoe       IN      A       172.16.12.3
jerboas         IN      A       172.16.12.4
ora             IN      A       172.16.1.2
;       host table has BOTH host and gateway entries for 10.104.0.19
wtb-gw          IN      A       10.104.0.19
;
;    Glue records for servers within this domain
;
linuxmag.articles  IN      A       172.16.18.15
24seven.events     IN      A       172.16.6.1
;
;       Define sub-domains
;
articles           IN      NS      linuxmag.articles.wrotethebook.com.
                   IN      NS      horseshoe.wrotethebook.com.
events             IN      NS      24seven.events.wrotethebook.com.
                   IN      NS      linuxmag.articles.wrotethebook.com.
```

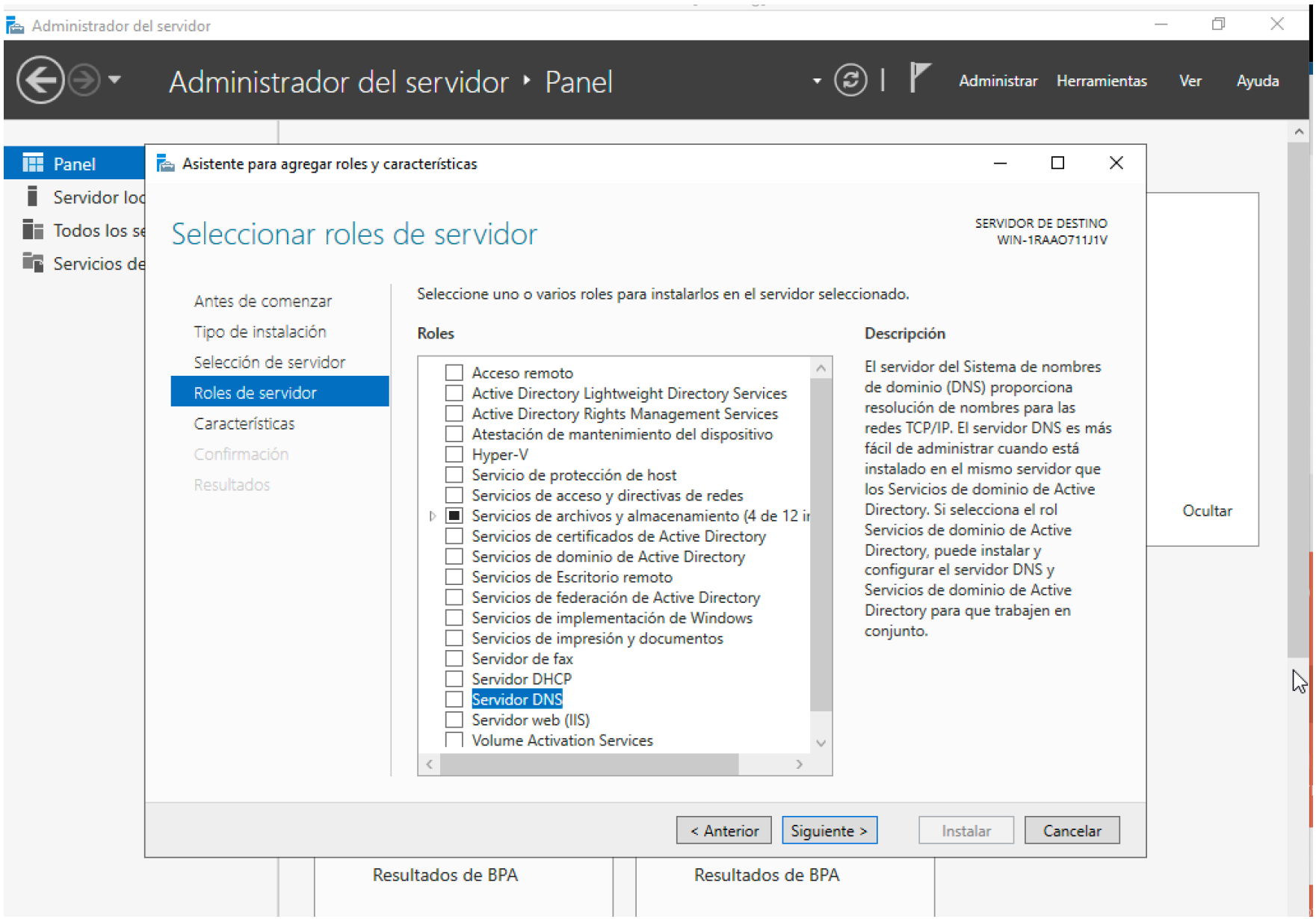
5.L Fichero de búsqueda inversa

- El primer registro es SOA. La @ hace referencia al origen actual; como no se ha incluido un comando $ORIGIN esta es 16.172.in-addr.arpa definido en named.conf

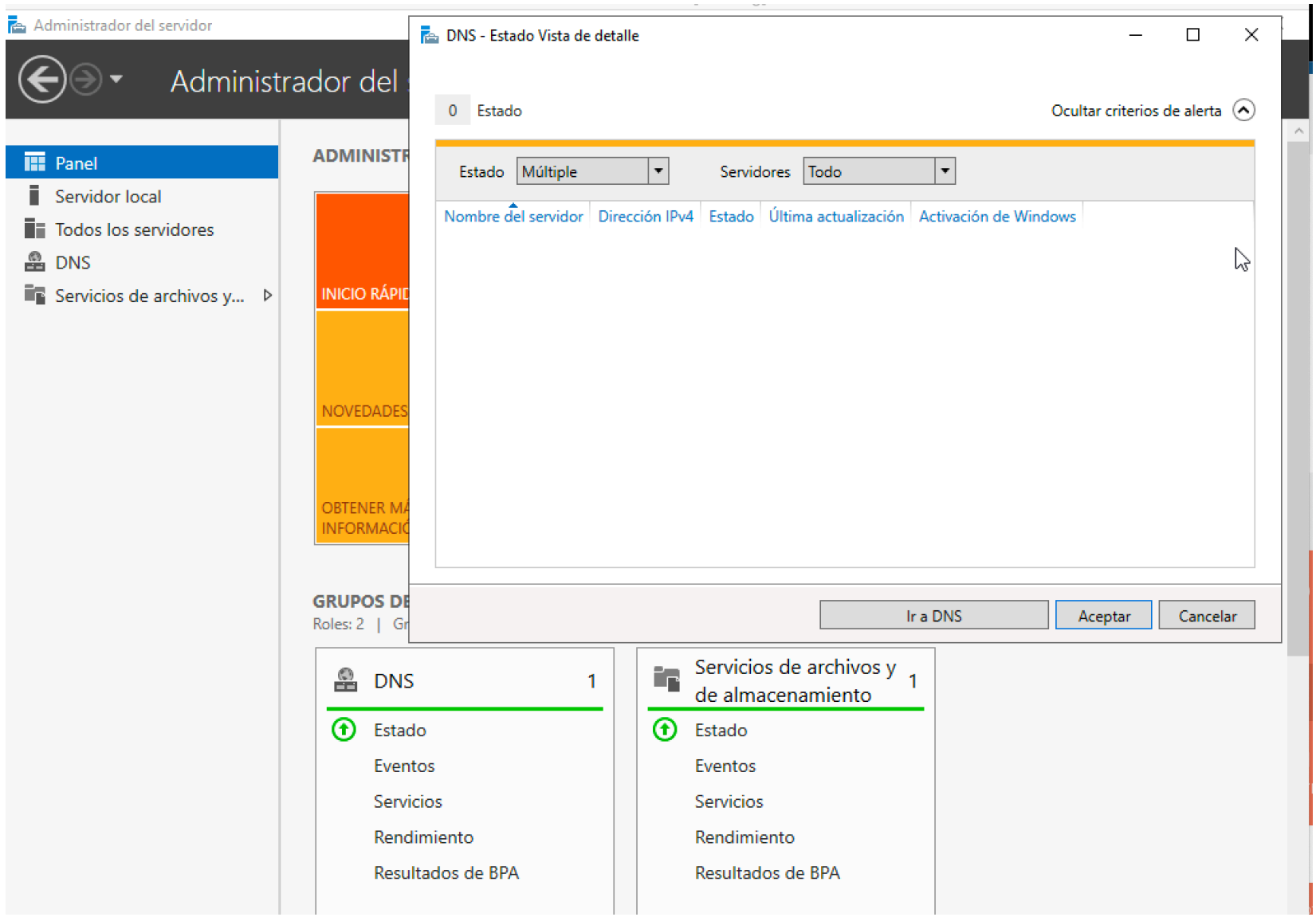
```
zone "16.172.in-addr.arpa" {
        type master;
        file "172.16.rev";
};
```

- Los registros NS que siguen a SOA definen los servidores de nombre del dominio. Observa que tienen el nombre en blanco, porque el último dominio sigue vigente
- Los registros PTR proporcionan los nombres de los hosts 12.1, 12.2, 12.3, 12.4 y 2.1 en la red 172.16. No terminan en punto, luego son relativos al dominio actual
- Los dos últimos registros crean subdominios

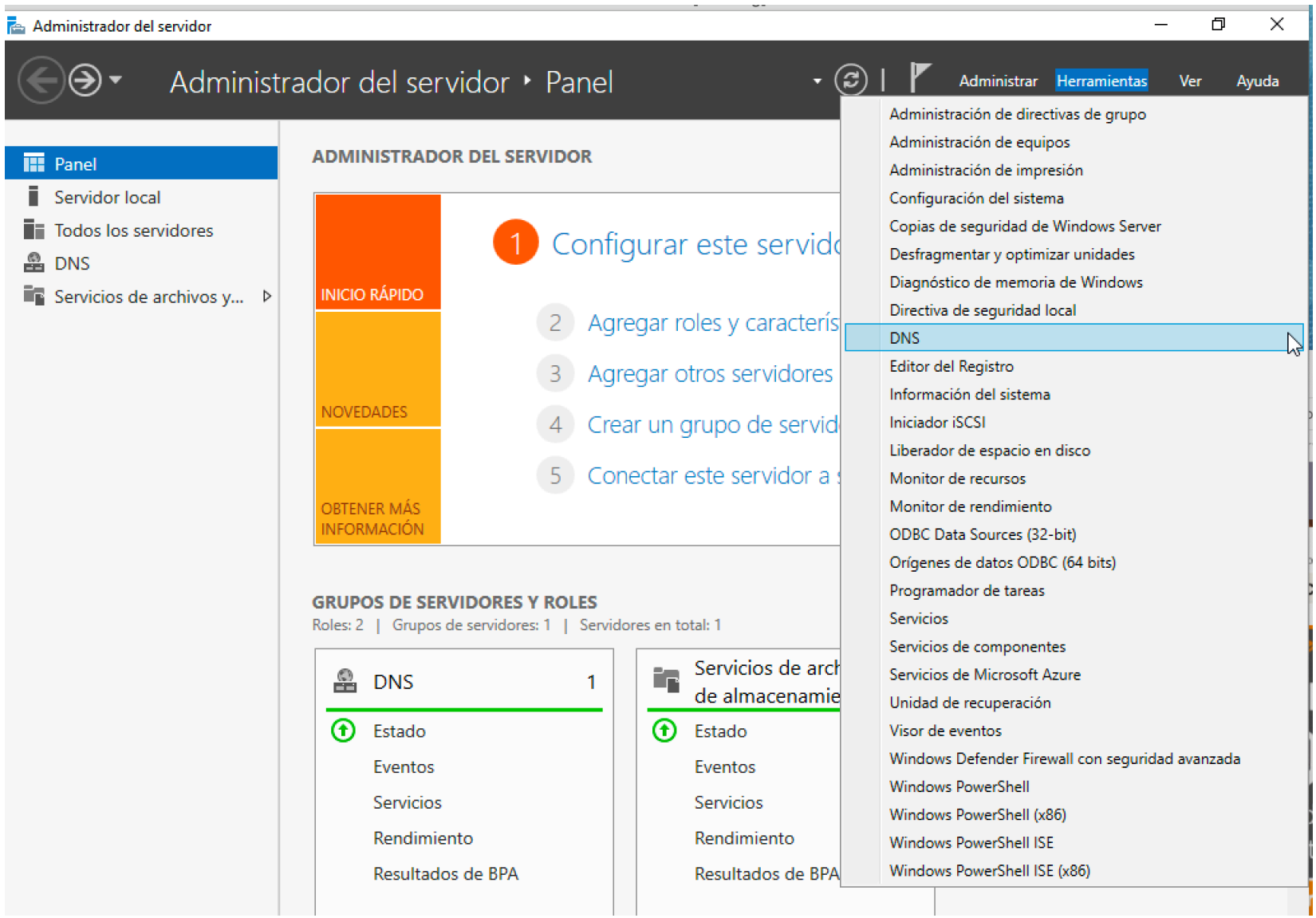
5.W Instalación servidor DNS Windows 2019



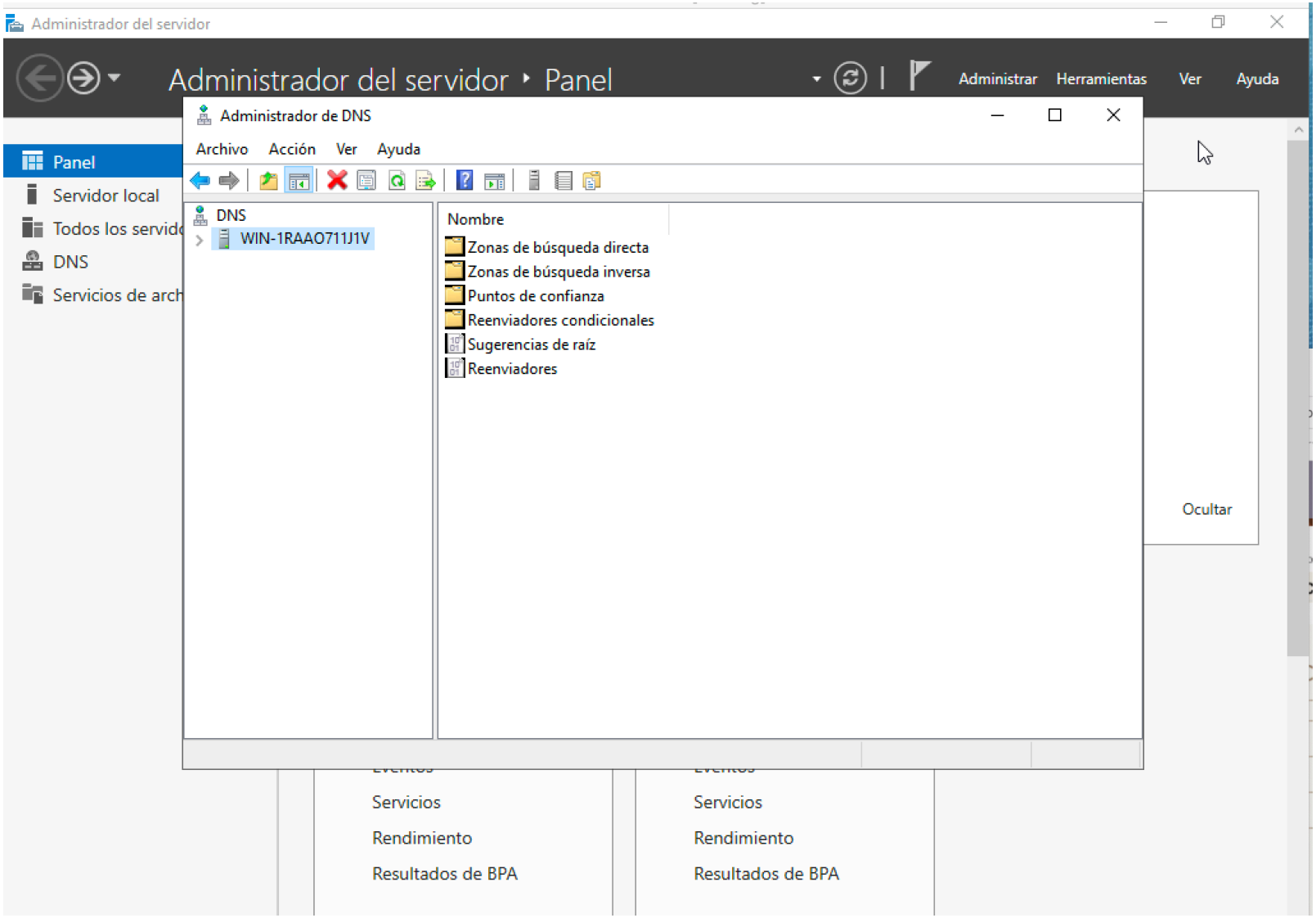
5.W Instalación servidor DNS Windows 2019



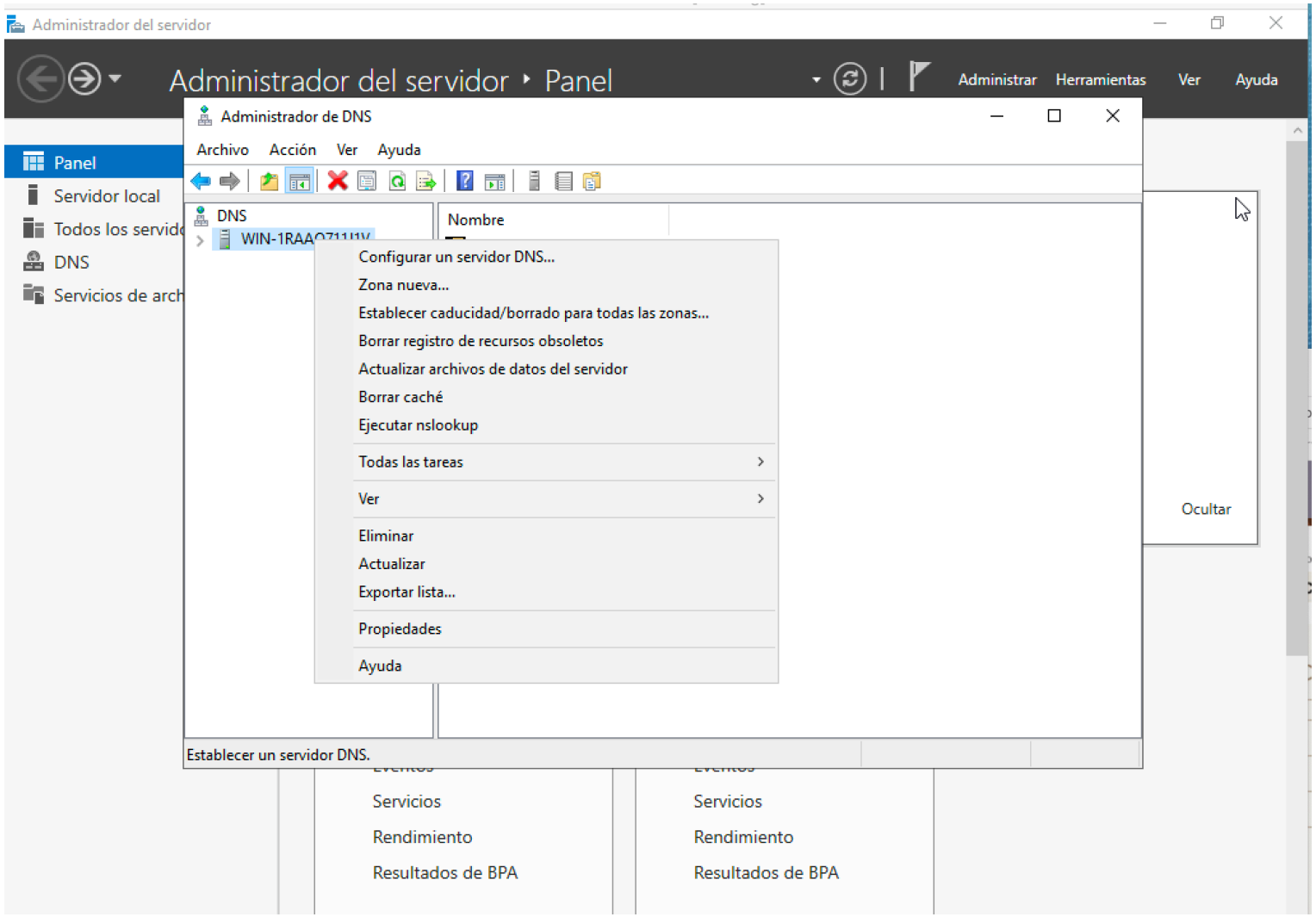
5.W Configuración servidor DNS Windows 2019



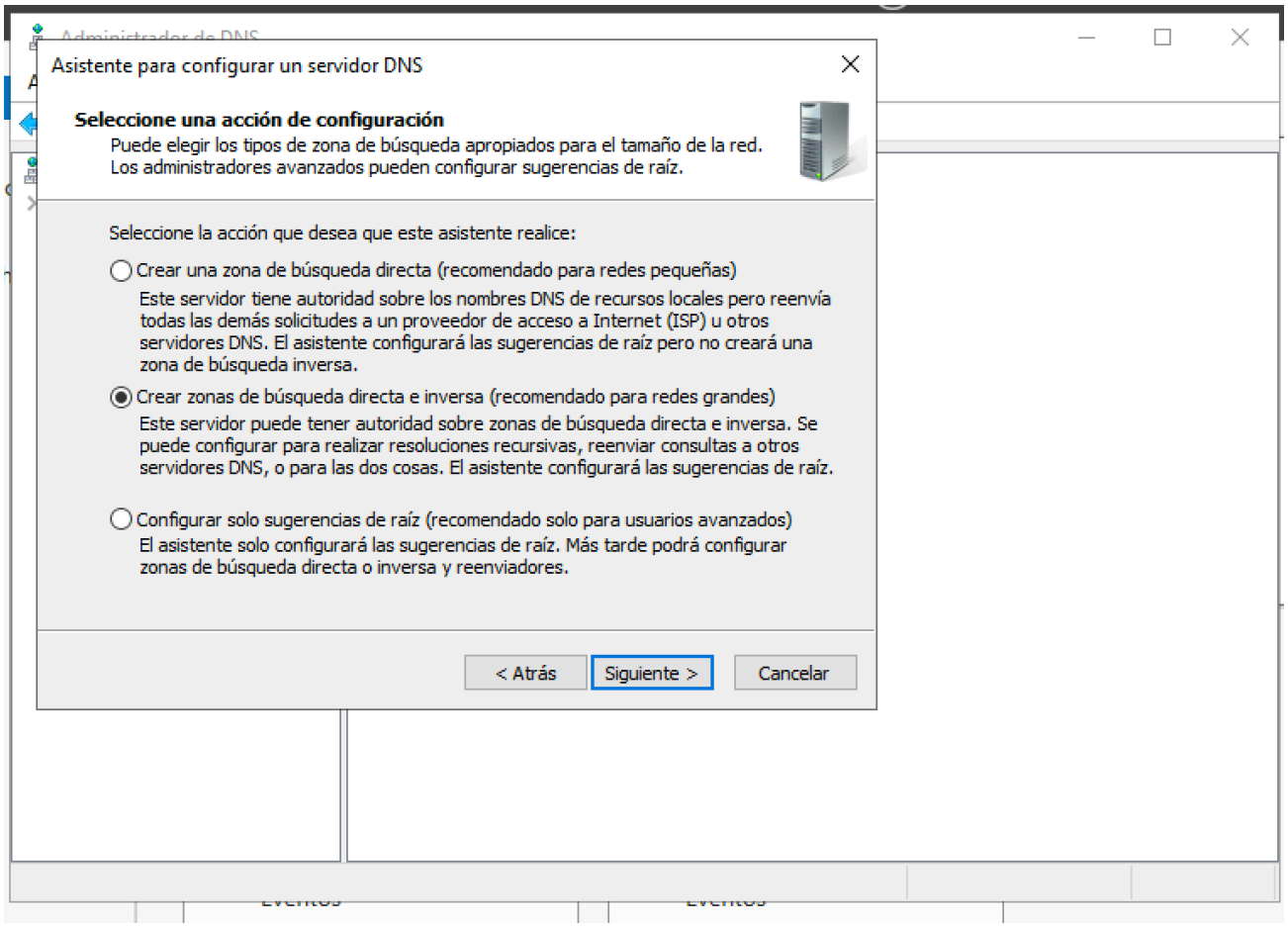
5.W Configuración servidor DNS Windows 2019



5.W Configuración servidor DNS Windows 2019

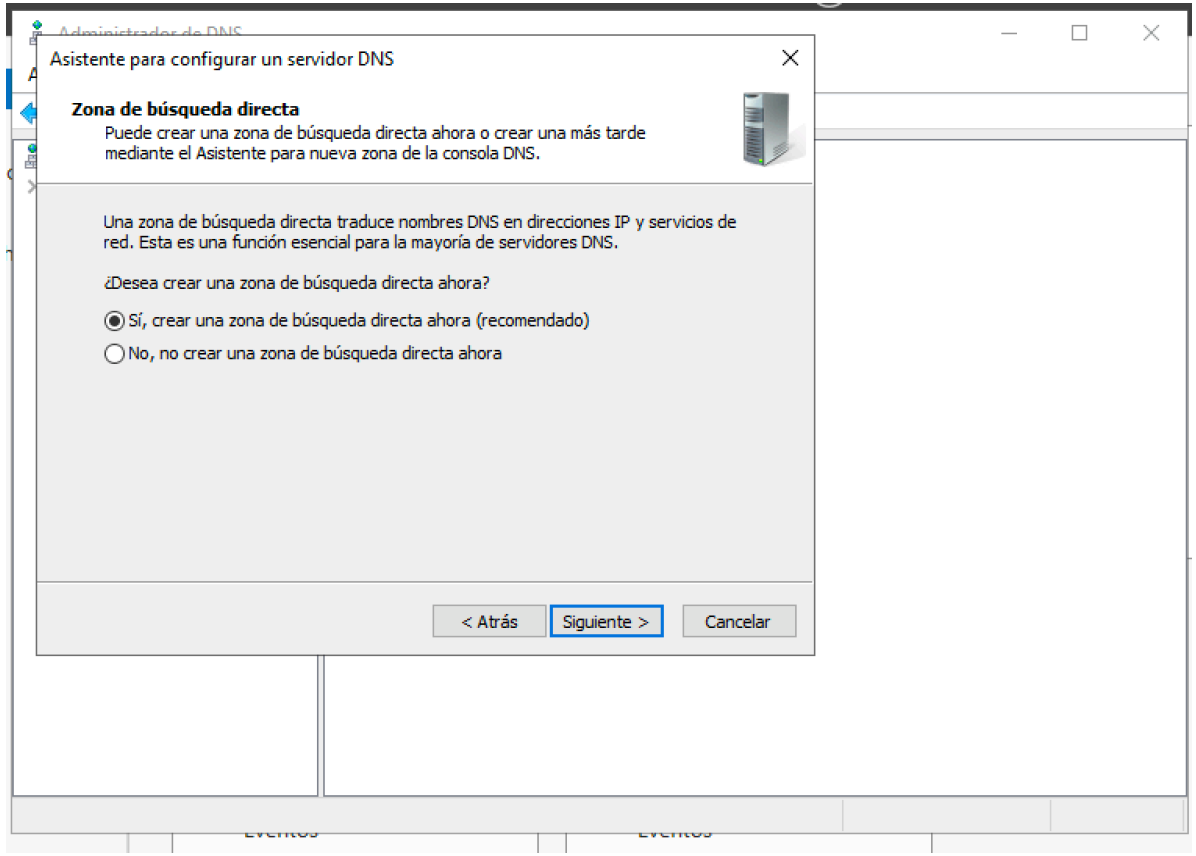


5.W DNS Windows



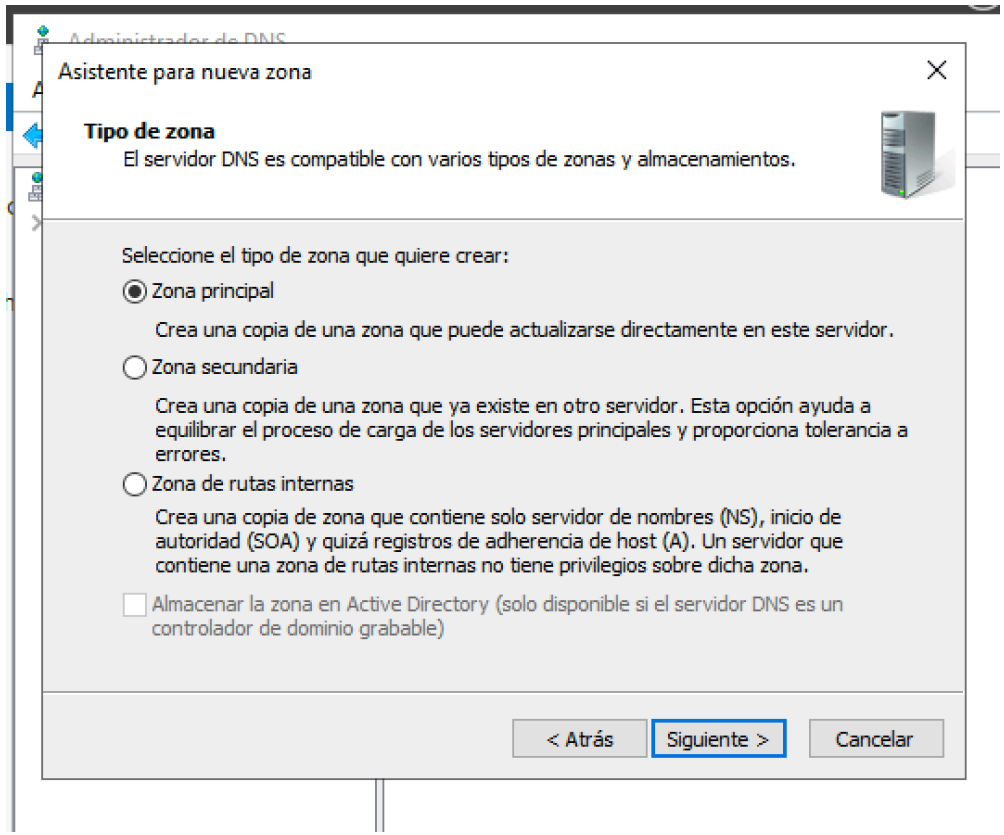
- El asistente permite crear zonas directa, inversa o sólo cache (sugerencias de raíz)

5.W DNS Windows



- Los ficheros de búsqueda con los registros de recursos se crean automáticamente

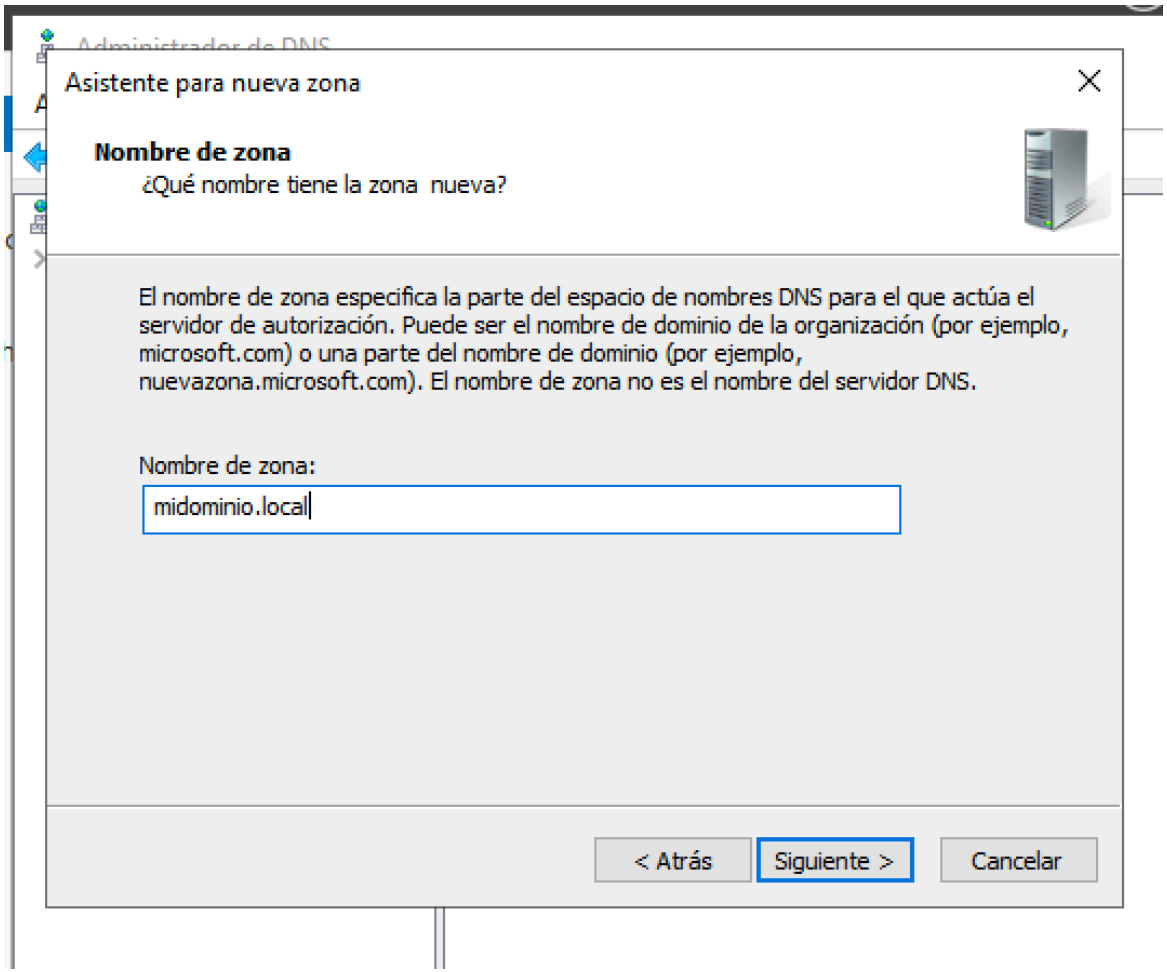
5.W DNS Windows



- La configuración de un DNS primario incluye, además de los ficheros con las sugerencias para la zona raíz y loopback, las directivas de zona para las que el servidor es autoridad

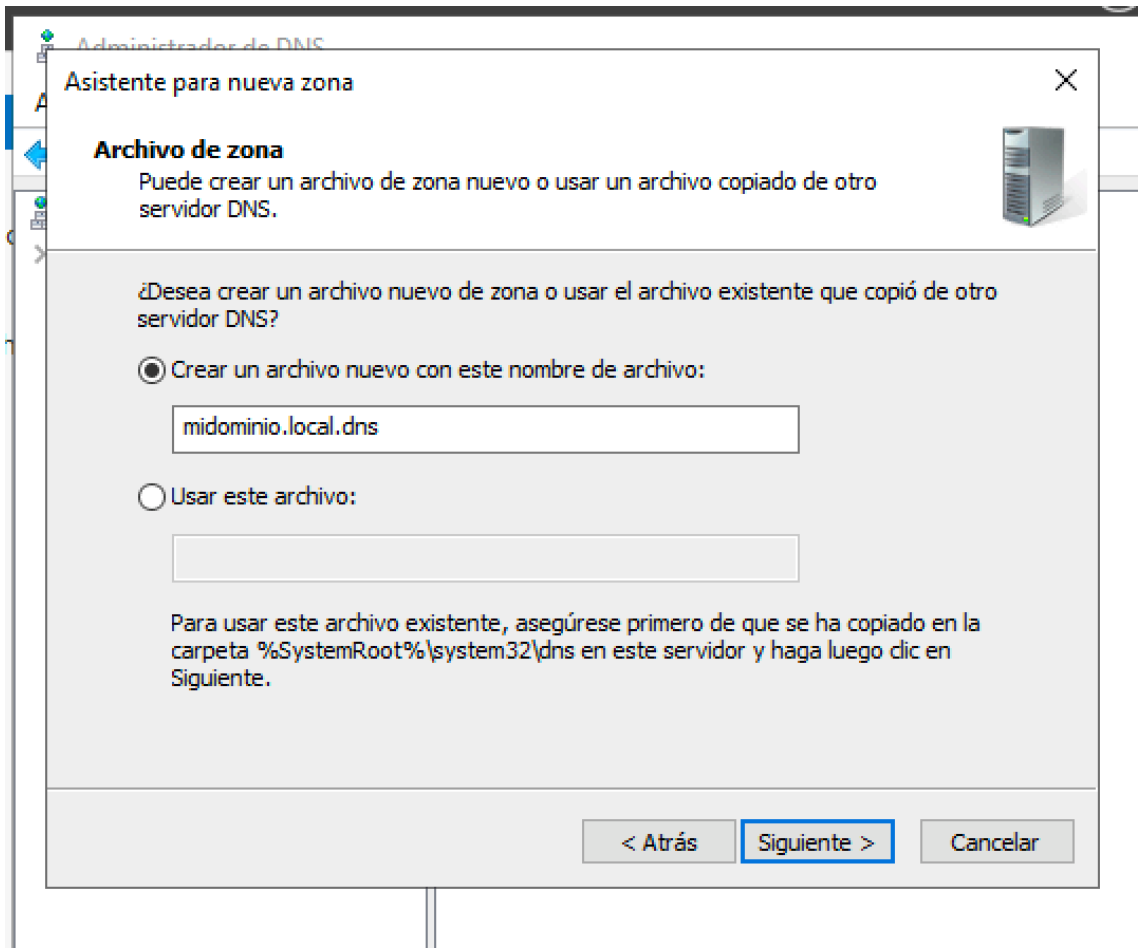
- En un DNS secundario, basta con indicarle la dirección del primario

5.W DNS Windows



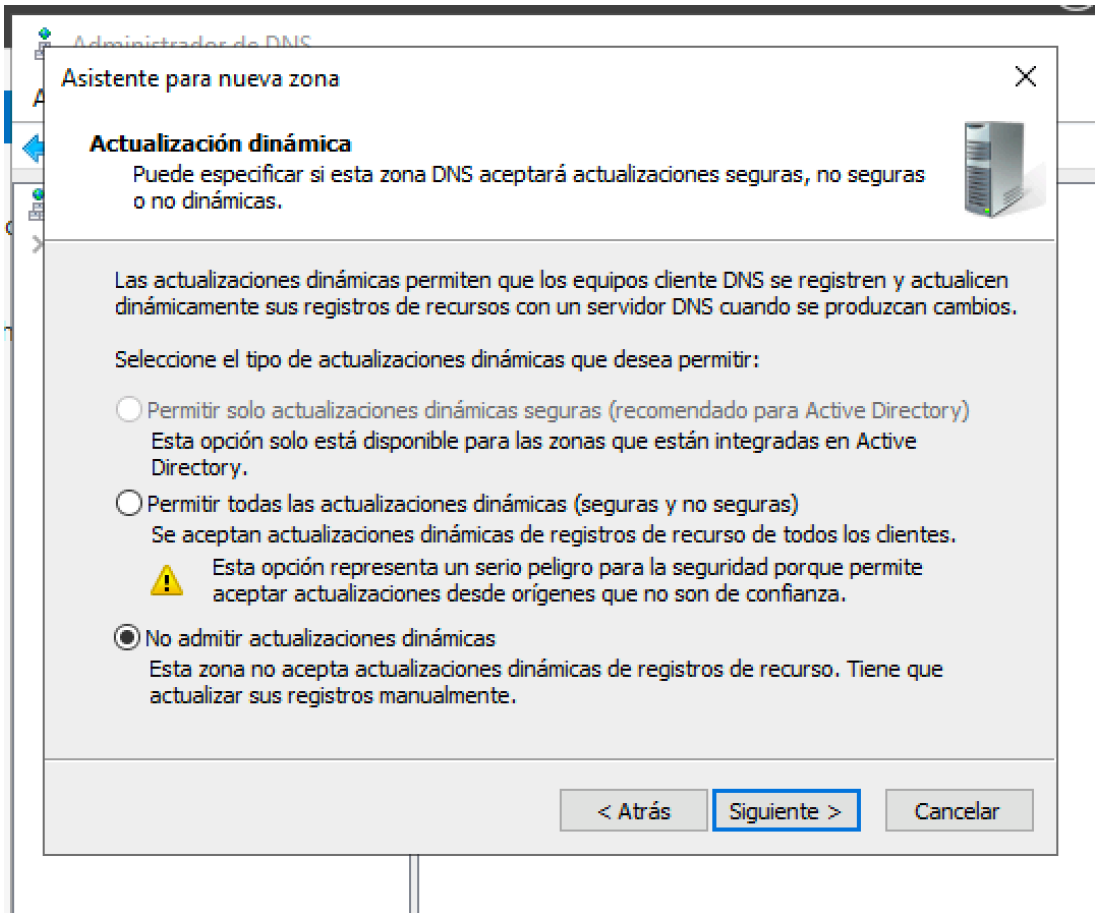
- El nombre de la zona puede elegirse libremente si el DNS no va a conectarse a Internet. En caso contrario, hay que registrar el dominio en el ISP

5.W DNS Windows



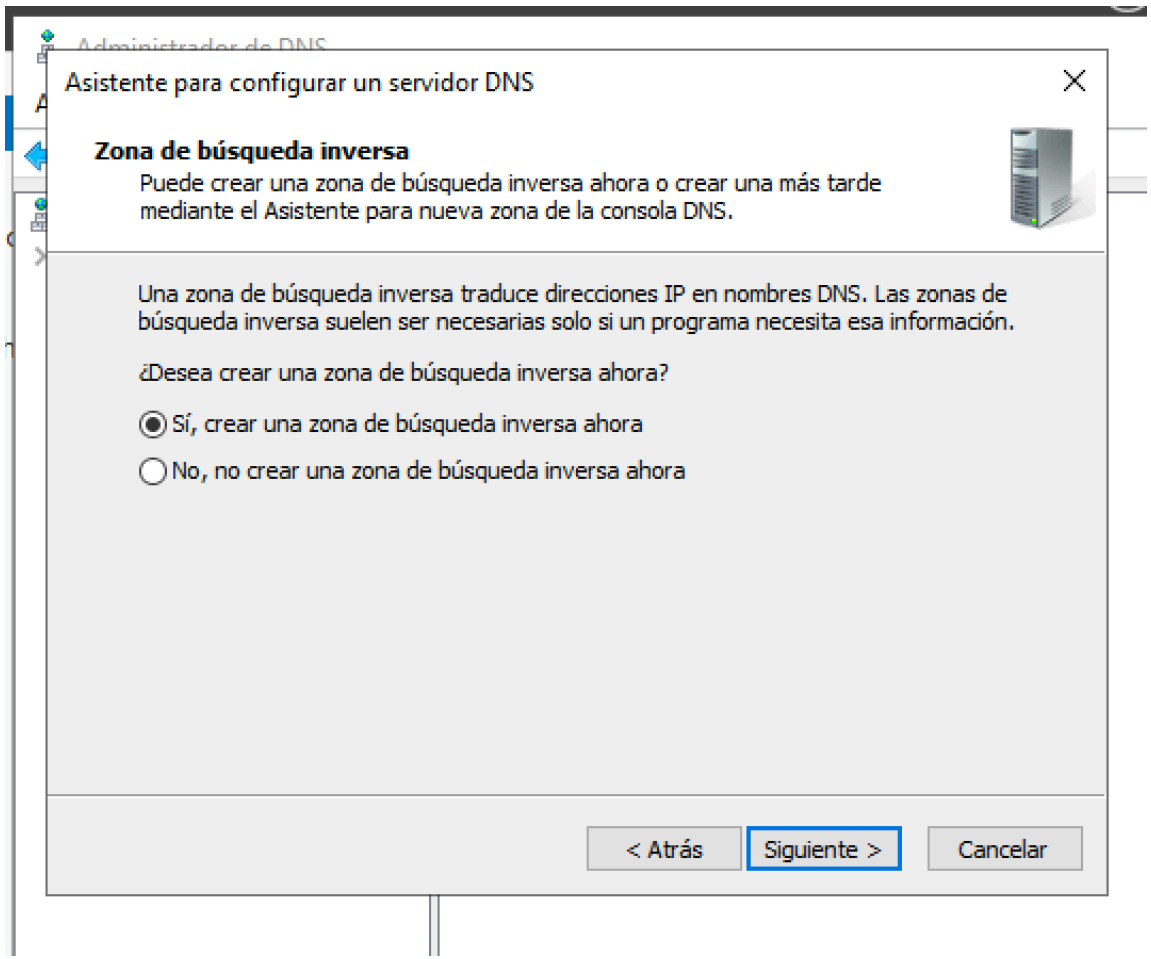
- El nombre por defecto del fichero donde se almacenan los registros de recurso es el mismo que el nombre de la zona, con sufijo .dns

5.W DNS Windows



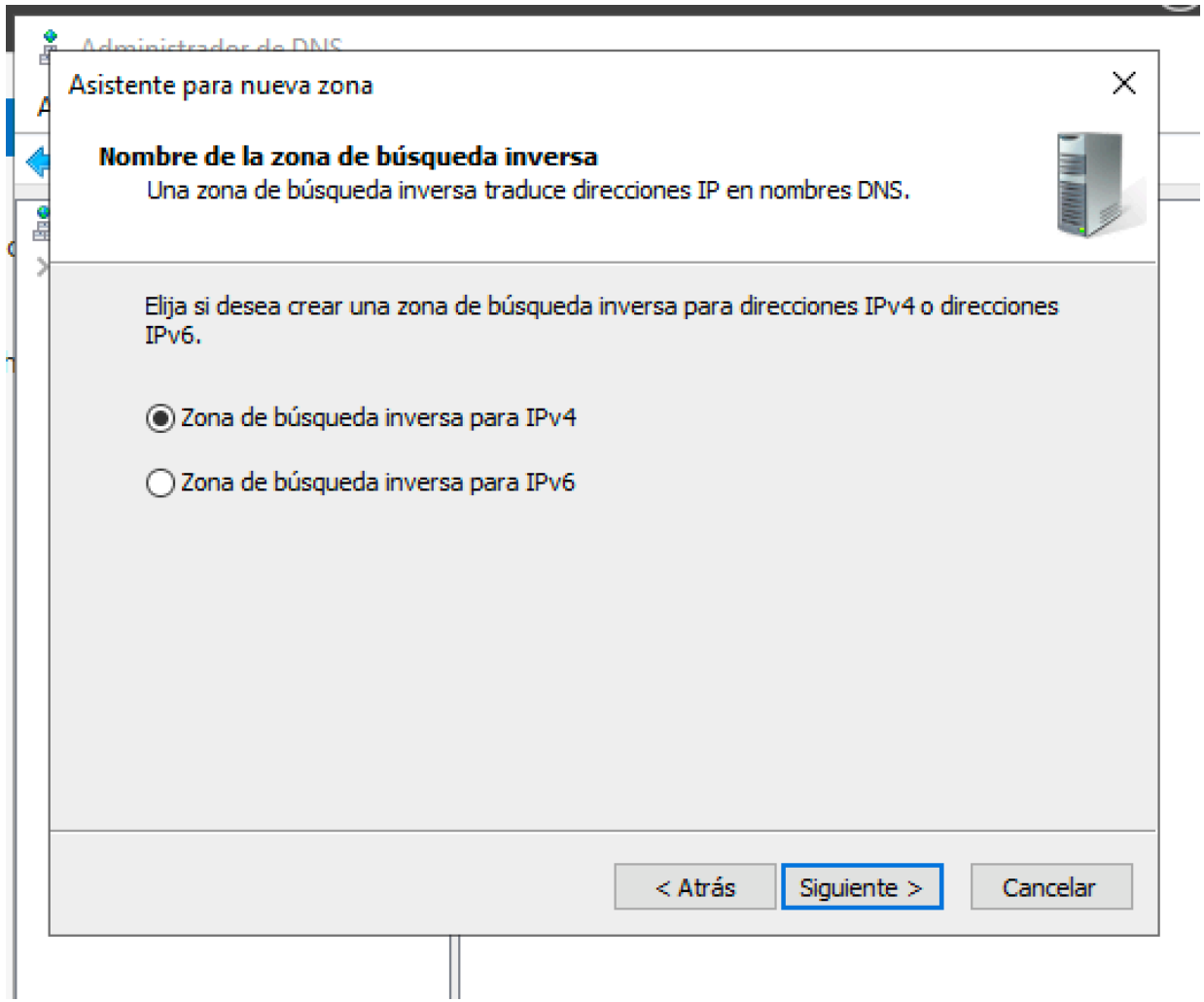
- En Windows se permiten actualizaciones dinámicas de la base de datos DNS
- Potencialmente es un problema de seguridad, es habitual no permitir la actualización

5.W DNS Windows



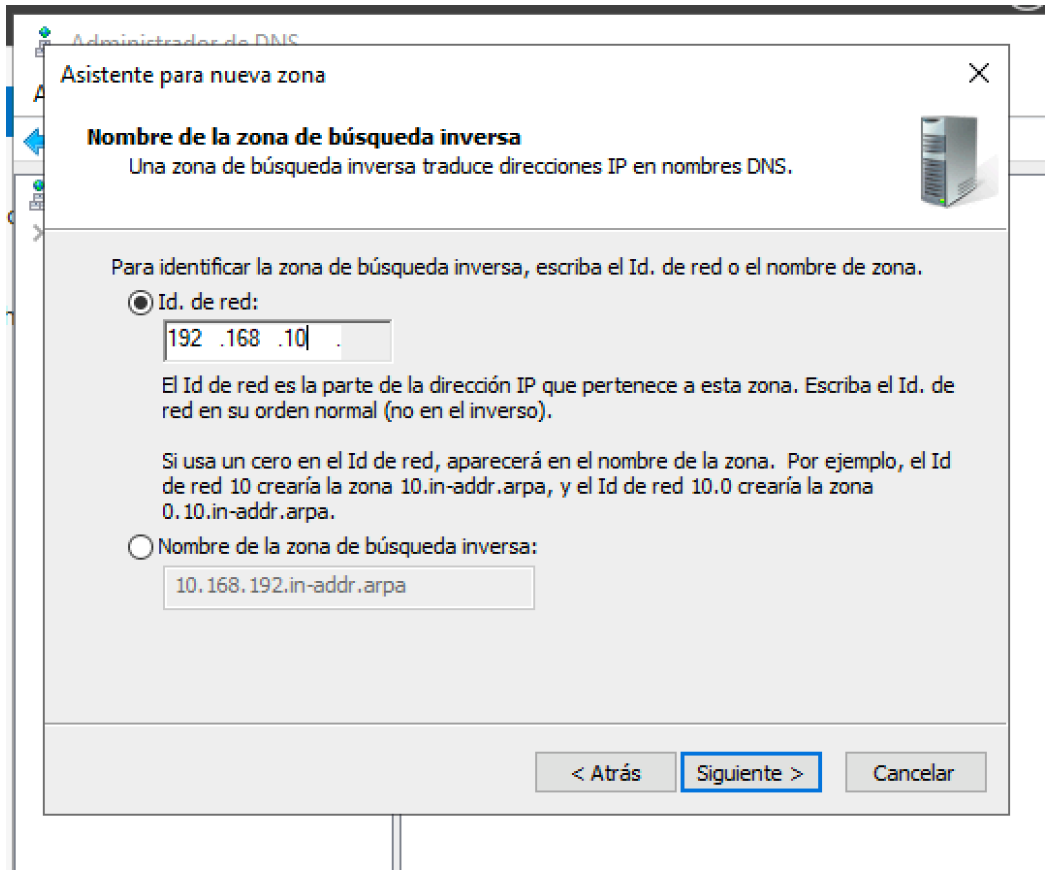
- El fichero de búsqueda inversa también se genera automáticamente con las directivas mínimas (SOA, etc.)

5.W DNS Windows



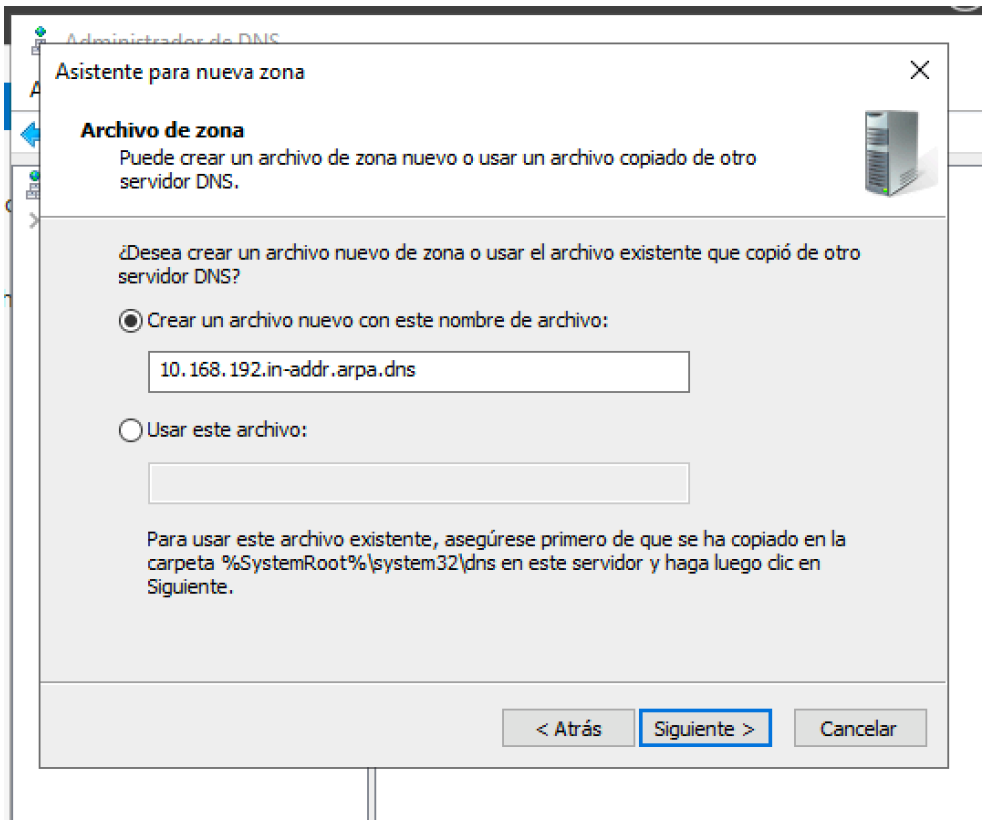
- Tras preguntar nuevamente el tipo de zona, se decide si la zona de búsqueda inversa es para IPV4 o IPV6

5.W DNS Windows



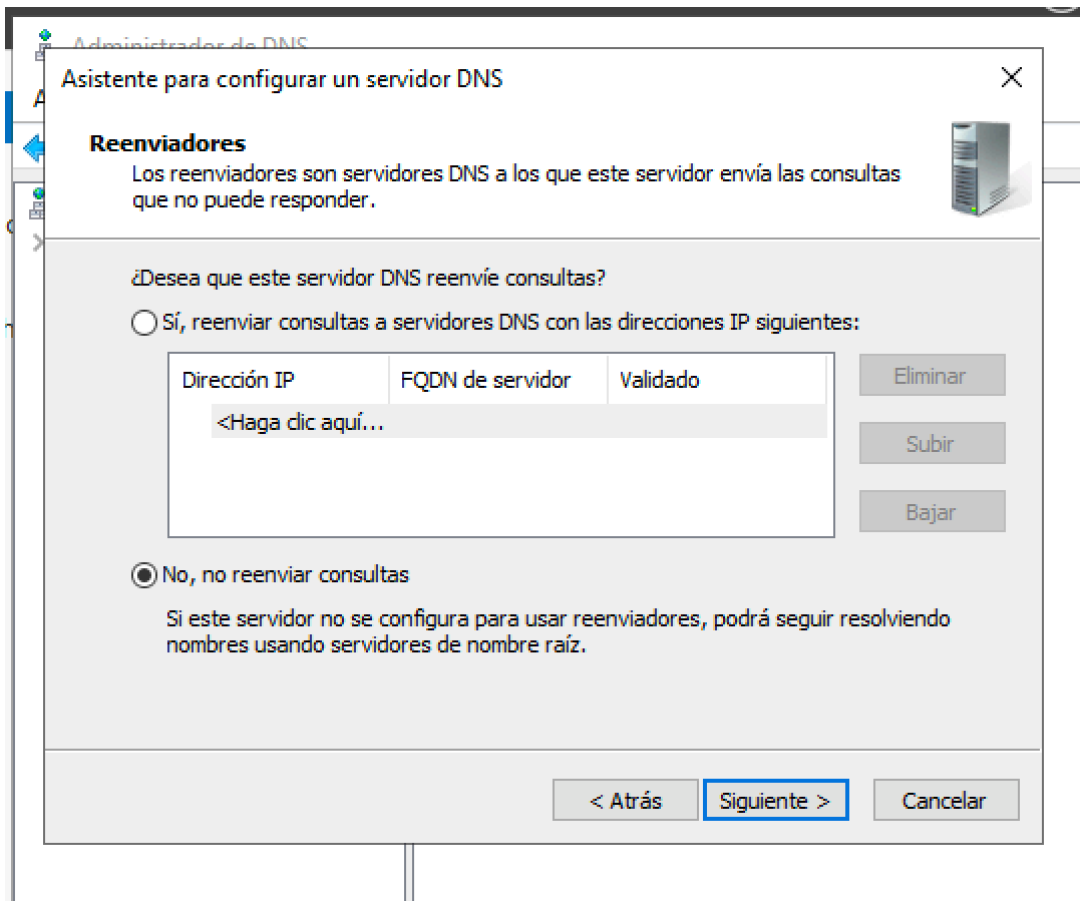
- La zona inversa tiene como nombre la dirección IP de la red asociada al dominio (sin la parte de host a ceros), seguida de in-addr.arpa

5.W DNS Windows



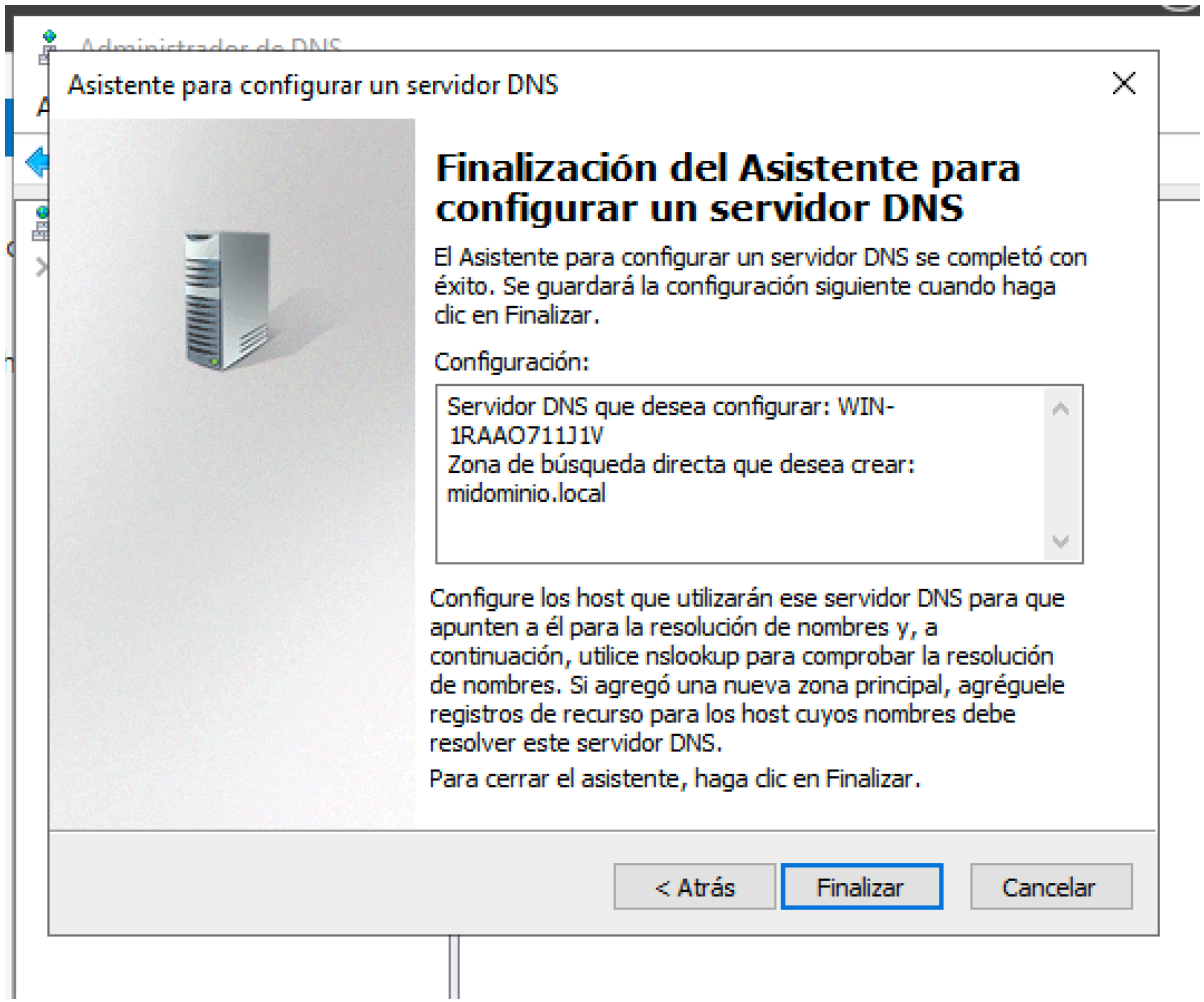
- El nombre del archivo de zona de nuevo es el mismo que el indicado en la directiva zone, con el sufijo .dns

5.W DNS Windows



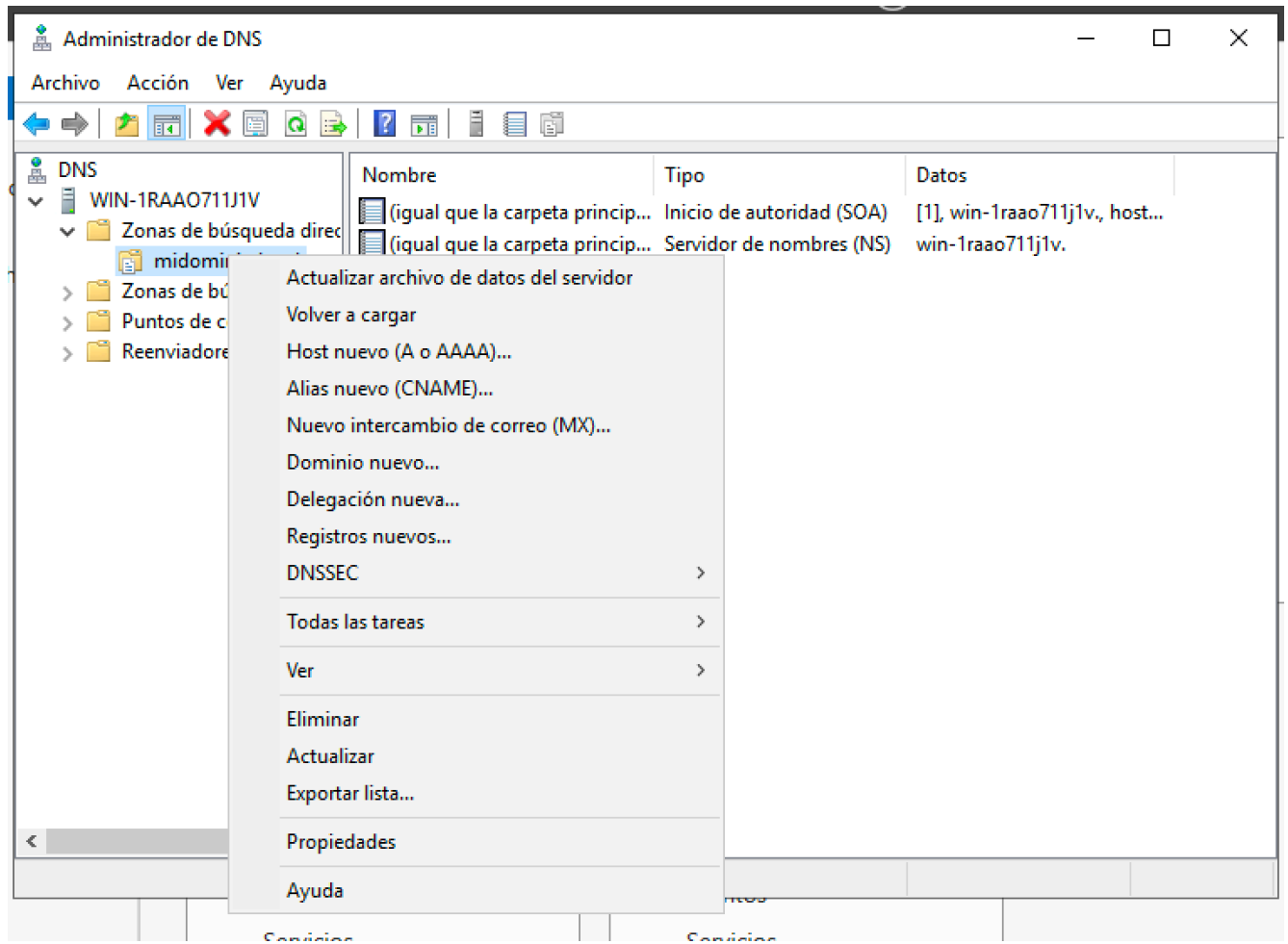
- Tras indicar si se desean actualizaciones dinámicas en la zona inversa, se le puede indicar al servidor que reenvíe sus consultas a otro servidor remoto, como se ha visto en la opción forwarders de BIND

5.W DNS Windows



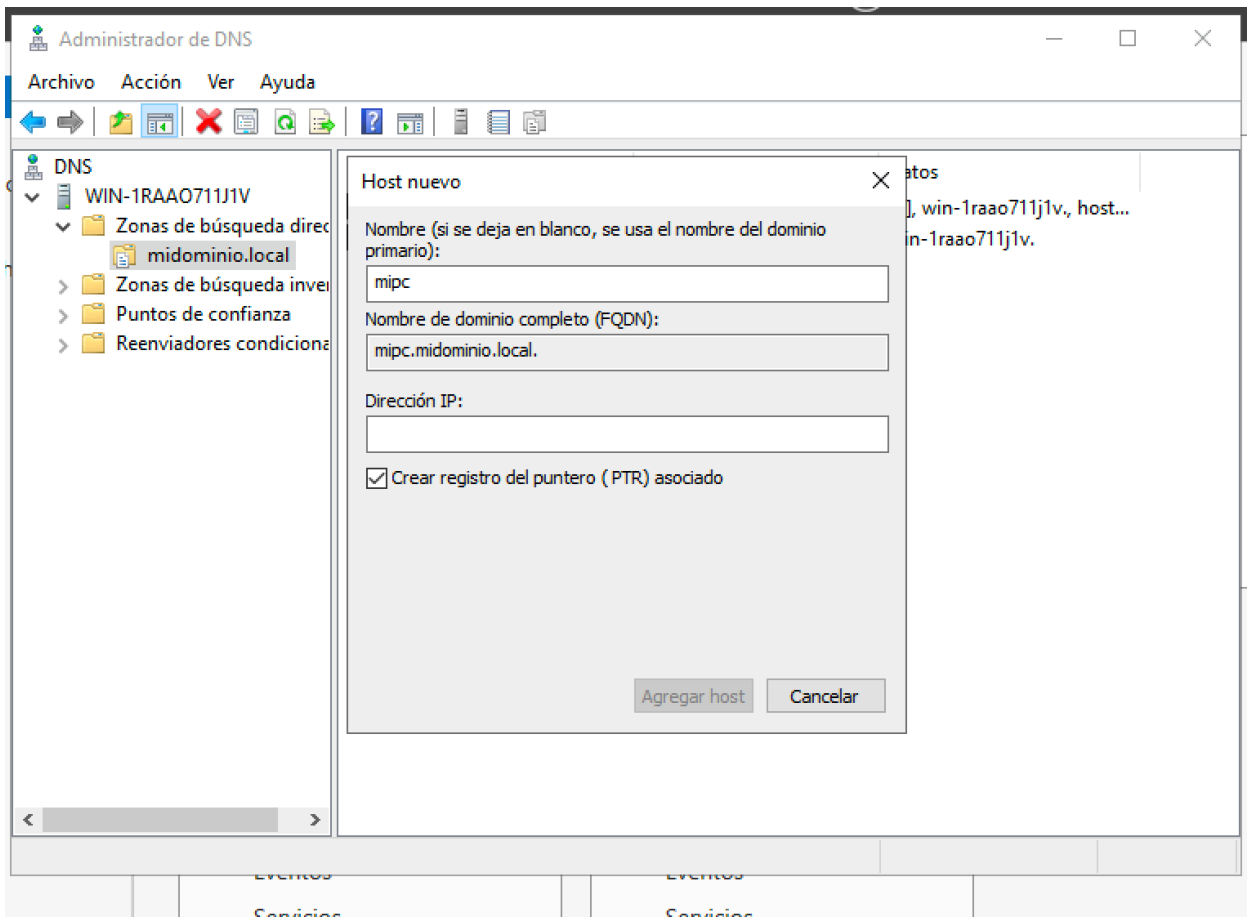
- El servidor se conecta automáticamente a la red y descarga el fichero de sugerencias raíz, como hemos hecho a mano con ftp en la versión linux

5.W DNS Windows



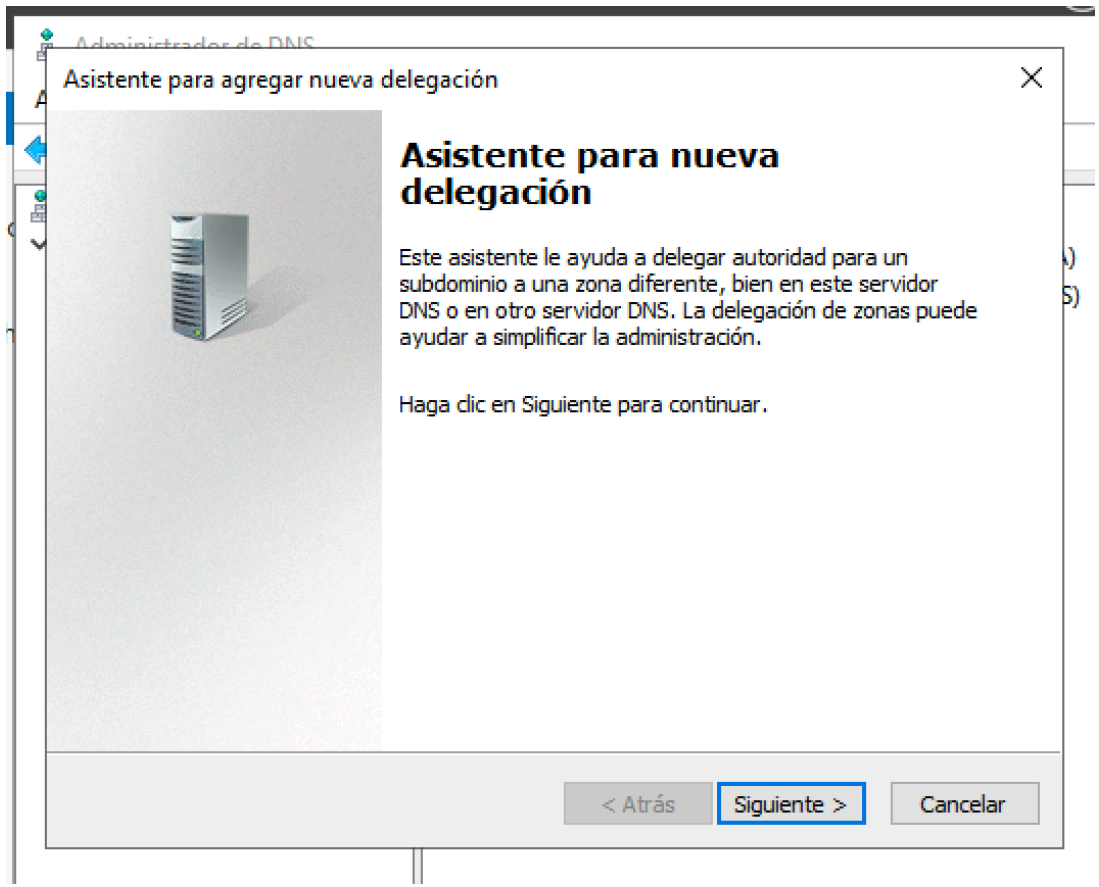
- Una vez creados todos los ficheros, se lanza la herramienta de administración y se introducen los contenidos

5.W DNS Windows



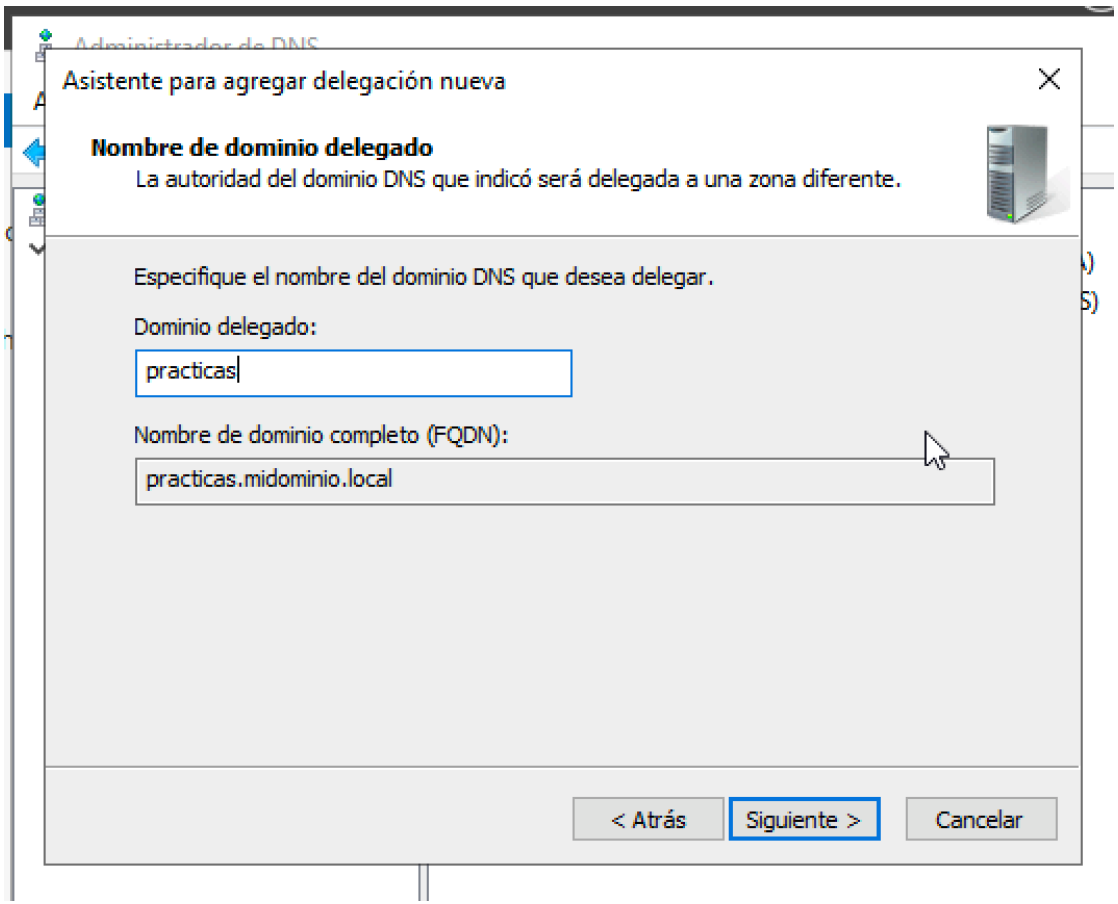
- Cada host se añade como un par nombre - dirección, y se puede incluir simultáneamente en la zona directa y en la inversa

5.W DNS Windows



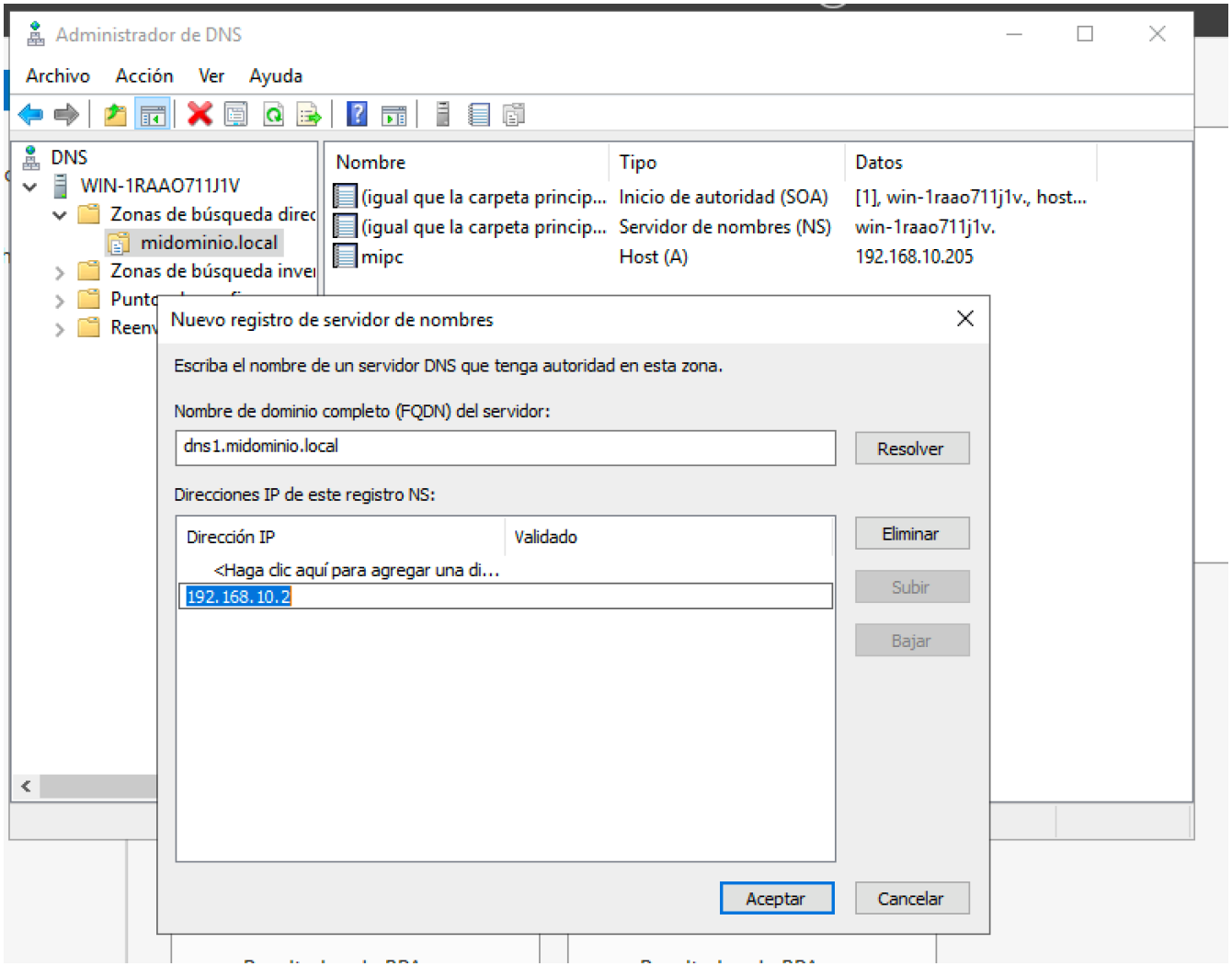
- Para crear subdominios es necesario indicar el nombre de los servidores DNS del subdominio en el dominio principal (registros NS)

5.W DNS Windows



- El dominio delegado tiene que pertenecer al dominio principal, y se gestionan un subconjunto de las direcciones IP asociadas al primero

5.W DNS Windows



- Puede haber más de un servidor DNS en un subdominio. Cada uno de ellos se da de alta indicando nombre y dirección IP