

PRÁCTICA 03

Servicio de nombres de dominio

Alexis Coves
Berna DAW
2ºW Grupo 2

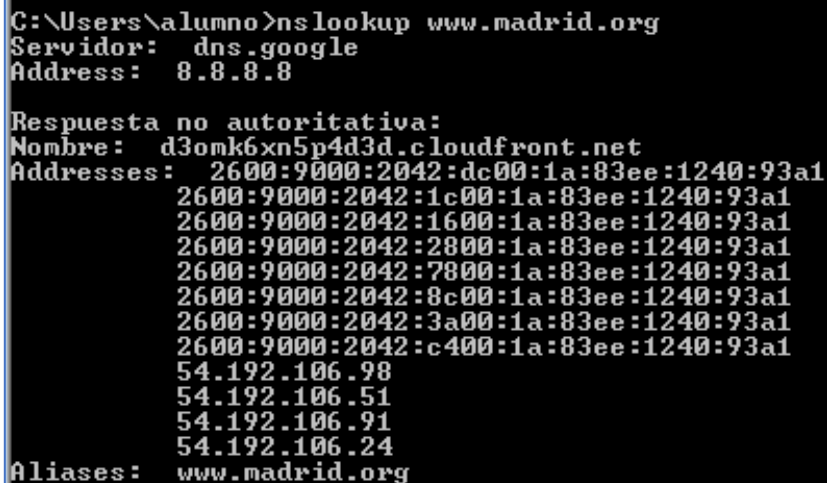
Índice:

3.1 Funcionamiento del servicio DNS	2
3.2 Instalación y configuración del servidor DNS como solo caché en Microsoft Windows 2008 Server	7
3.3 Servidor DNS en Microsoft Windows Server 2008. Configuración del servidor como primario (maestro) para una zona de resolución directa .	12
3.4 Servidor DNS en Microsoft Windows Server 2008. Configuración del servidor como primario (maestro) para una zona inversa	19
3.8 Cliente DNS en las otras máquinas	25

3.1 Funcionamiento del servicio DNS

En este apartado usaremos los comandos “nslookup” y “dig” para obtener información y verificar el funcionamiento de los servidores.

Windows 7



```
C:\Users\alumno>nslookup www.madrid.org
Servidor:  dns.google
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:  d3onk6xn5p4d3d.cloudfront.net
Addresses:  2600:9000:2042:dc00:1a:83ee:1240:93a1
           2600:9000:2042:1c00:1a:83ee:1240:93a1
           2600:9000:2042:1600:1a:83ee:1240:93a1
           2600:9000:2042:2800:1a:83ee:1240:93a1
           2600:9000:2042:7800:1a:83ee:1240:93a1
           2600:9000:2042:8c00:1a:83ee:1240:93a1
           2600:9000:2042:3a00:1a:83ee:1240:93a1
           2600:9000:2042:c400:1a:83ee:1240:93a1
           54.192.106.98
           54.192.106.51
           54.192.106.91
           54.192.106.24
Aliases:  www.madrid.org
```

Ejecutamos el comando “nslookup www.madrid.org” para obtener las direcciones IP asociadas al nombre DNS.

Comprobamos que la respuesta nos la proporciona el servidor DNS público de Google configurado anteriormente en el protocolo TCP/IP.

Comprobamos que existen distintas IPs asociadas al nombre de dominio. Esto se debe a que el dominio utiliza la técnica DNS Round Robin que sirve para la distribución y reducción de la carga, además de tolerancia a fallos y aprovisionamiento múltiple y redundante para las peticiones del cliente hacia el servidor.

Observamos que el nombre equivalente o alias es “www.madrid.org”.

Observamos que la respuesta es no autoritativa, esto indica que el servidor DNS local no puede responder a la consulta por sí solo, sino que ha debido contactar a uno o varios servidores de nombres alternativos. Es decir, el servidor DNS 8.8.8.8 no gestiona la zona autoritaria en la que se encuentra la dirección “www.madrid.org”.

```
C:\Users\alumno>nslookup 130.206.13.20
Servidor:  dns.google
Address:  8.8.8.8

Nombre:   www.rediris.es
Address:  130.206.13.20

C:\Users\alumno>_
```

Ejecutamos el comando "nslookup 130.206.13.20" para obtener los nombres de dominio asociados a dicha dirección IP.

```
C:\Users\alumno>nslookup www.madrid.org 8.8.4.4
Servidor:  dns.google
Address:  8.8.4.4

Respuesta no autoritativa:
Nombre:   d3omk6xn5p4d3d.cloudfront.net
Addresses: 2600:9000:2042:800:1a:83ee:1240:93a1
           2600:9000:2042:a000:1a:83ee:1240:93a1
           2600:9000:2042:fa00:1a:83ee:1240:93a1
           2600:9000:2042:c600:1a:83ee:1240:93a1
           2600:9000:2042:9a00:1a:83ee:1240:93a1
           2600:9000:2042:5c00:1a:83ee:1240:93a1
           2600:9000:2042:4000:1a:83ee:1240:93a1
           2600:9000:2042:2e00:1a:83ee:1240:93a1
           54.192.106.91
           54.192.106.24
           54.192.106.98
           54.192.106.51
Alias:    www.madrid.org
```

Ejecutamos el comando "nslookup www.madrid.org 8.8.4.4" especificando que nos responda el servidor DNS público de Google 8.8.4.4.

Observamos que nos devuelve las mismas direcciones IP que en el caso anterior en el que nos respondía el servidor DNS 8.8.8.8.

```
C:\Users\alumno>nslookup www.madrid.org olimpia.madrid.org
Servidor:  ns2.comunidad.madrid
Address:  213.0.53.140

Nombre:   www.madrid.org

C:\Users\alumno>_
```

Ejecutamos el comando "nslookup www.madrid.org olimpia.madrid.org" para que nos responda el servidor DNS olimpia.madrid.org.

Observamos que nos responde el servidor DNS "ns2.comunidad.madrid" y esta vez sí es una respuesta autoritativa ya que el servidor DNS "olimpia.madrid.org" gestiona la zona autoritaria en la que se encuentra la dirección "www.madrid.org".

Linux

```
alumno@ServidorLinux21:~$ nslookup www.google.es
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   www.google.es
Address: 216.58.201.131

alumno@ServidorLinux21:~$ _
```

Ejecutamos el comando "nslookup www.google.es" para obtener la dirección IP.

Observamos que a pesar de que tenemos configurado el servidor DNS público de Google 8.8.8.8, este no gestiona la zona autoritaria en la que se encuentra la dirección www.google.es, con lo cual la respuesta es no autoritativa.

```
alumno@ServidorLinux21:~$ dig www.google.es

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> www.google.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43902
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.google.es.                IN      A

;; ANSWER SECTION:
www.google.es.                139     IN      A      172.217.168.163

;; Query time: 44 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Nov 12 10:56:43 CET 2020
;; MSG SIZE rcvd: 58

alumno@ServidorLinux21:~$ _
```

Ejecutamos el comando "dig www.google.es" para obtener la/s direcciones IP asociadas al servidor DNS.

A diferencia de nslookup, el comando dig nos proporciona una información mucho más detallada como, un pequeño resumen con la pregunta y la respuesta, además del tiempo de ejecución de la petición en milisegundos, el puerto que la ha realizado, la fecha y la hora y el tamaño.

```

alumno@ServidorLinux21:~$ dig -x 130.206.13.20

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> -x 130.206.13.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56071
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;20.13.206.130.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
20.13.206.130.in-addr.arpa. 7199 IN      PTR      www.rediris.es.

;; Query time: 71 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Nov 12 10:58:47 CET 2020
;; MSG SIZE rcvd: 83

alumno@ServidorLinux21:~$ _

```

Ejecutamos el comando "dig -x 130.206.13.20" para obtener el nombre del dominio mediante la resolución inversa.

Como podemos observar en la pregunta, se invierte la dirección IP y se le añade el sufijo ".in-addr.arpa", un dominio especial para la resolución de búsqueda inversa.

```

alumno@ServidorLinux21:~$ dig @8.8.4.4 www.google.es

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> @8.8.4.4 www.google.es
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4403
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;www.google.es.                  IN      A

;; ANSWER SECTION:
www.google.es.                  189     IN      A          216.58.201.131

;; Query time: 69 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Thu Nov 12 11:00:31 CET 2020
;; MSG SIZE rcvd: 58

alumno@ServidorLinux21:~$ _

```

Ejecutamos el comando "dig @8.8.4.4 www.google.es" para obtener la/s direcciones IP asociadas al servidor DNS 8.8.4.4.

Observamos que seguimos teniendo una respuesta no autoritativa.

```
alumno@ServidorLinux21:~$ dig @ns1.google.com www.google.es

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> @ns1.google.com www.google.es
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53948
;; flags: qr aa rd: QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;www.google.es.                IN      A

;; ANSWER SECTION:
www.google.es.                300     IN      A      216.58.201.163

;; Query time: 69 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Thu Nov 12 11:02:33 CET 2020
;; MSG SIZE rcvd: 58

alumno@ServidorLinux21:~$ _
```

Ejecutamos el comando "dig @ns1.google.com www.google.es" para obtener la/s direcciones IP asociadas al servidor DNS ns1.google.com.

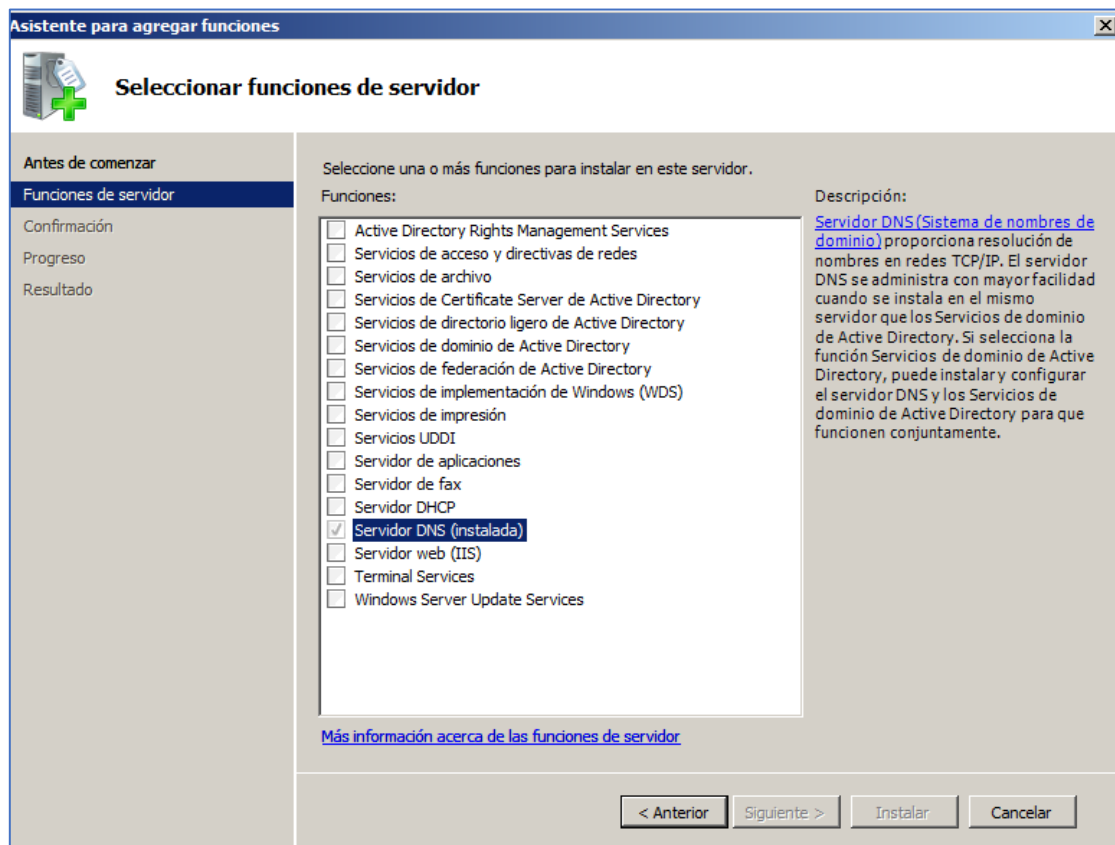
Observamos que sigue siendo una respuesta no autoritativa ya que la dirección www.google.es no está en la zona autoritaria que gestiona el servidor DNS ns1.google.com.

3.2 Servidor DNS en Microsoft Windows Server 2008.

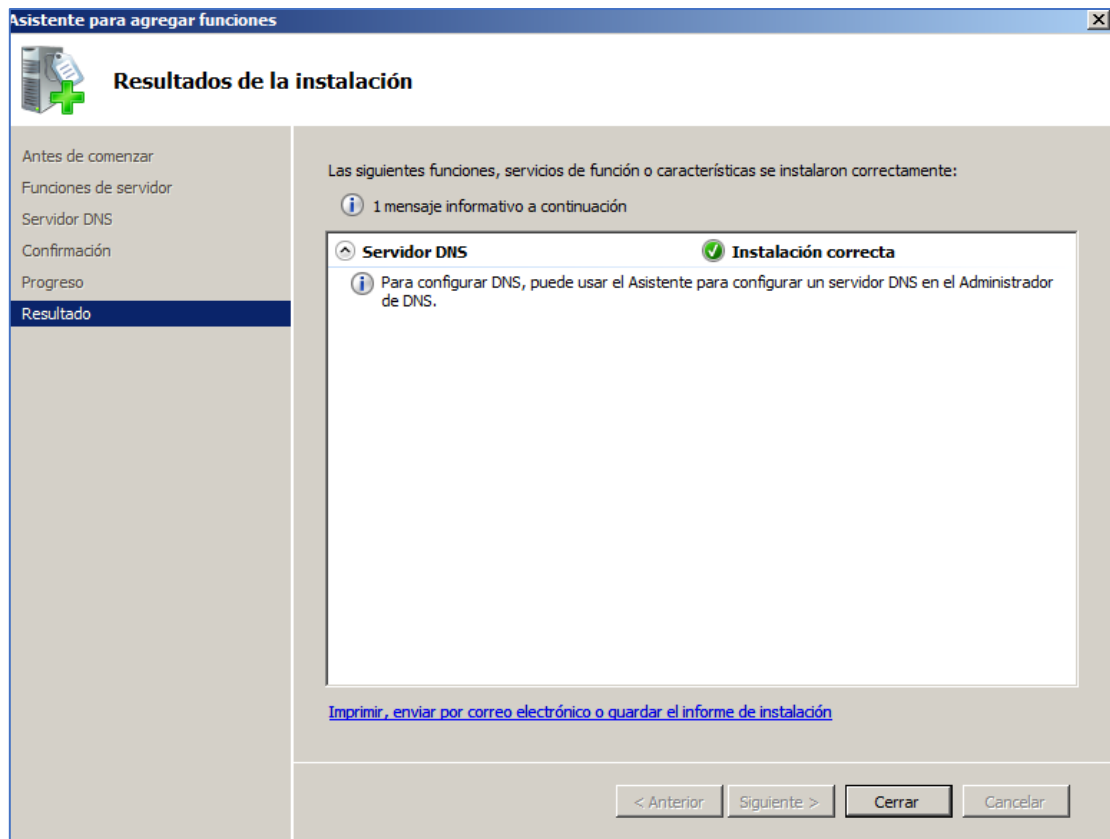
Instalación y configuración del servidor DNS como solo cache.

1. Instalación:

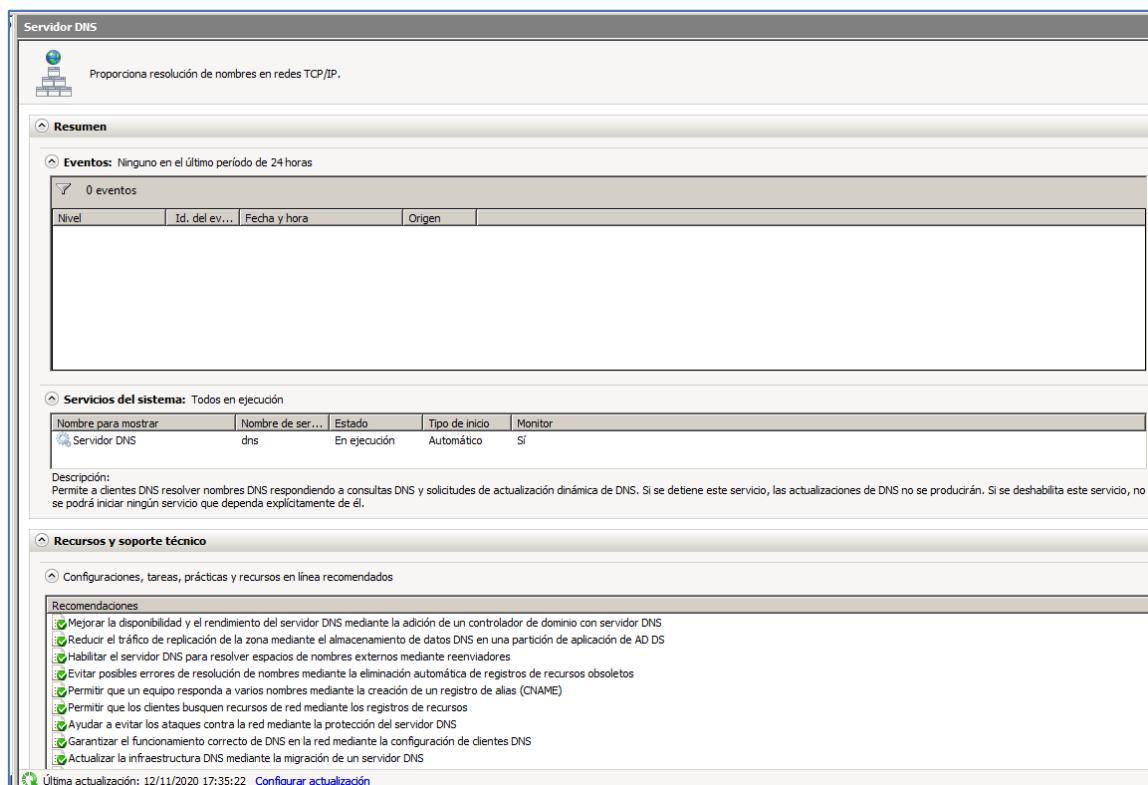
Para instalar el servicio DNS iremos al **Administrador del servidor** y seleccionaremos **Funciones**, a continuación en la ventana de la derecha haremos click en **Agregar Funciones**.



En el asistente, daremos a siguiente hasta llegar a la siguiente ventana, seleccionaremos Servidor DNS y pincharemos en instalar.



Configuración final del servicio DNS.



Información sobre eventos, servicios y recursos y soporte técnico del servidor.

```
C:\Users\Administrador>netstat -a -n -p TCP

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135           0.0.0.0:0             LISTENING
TCP    0.0.0.0:445           0.0.0.0:0             LISTENING
TCP    0.0.0.0:5357          0.0.0.0:0             LISTENING
TCP    0.0.0.0:49152         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49153         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49154         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49155         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49156         0.0.0.0:0             LISTENING
TCP    0.0.0.0:49157         0.0.0.0:0             LISTENING
TCP    127.0.0.1:53          0.0.0.0:0             LISTENING
TCP    192.168.8.22:53       0.0.0.0:0             LISTENING
TCP    192.168.8.22:139     0.0.0.0:0             LISTENING

C:\Users\Administrador>_
```

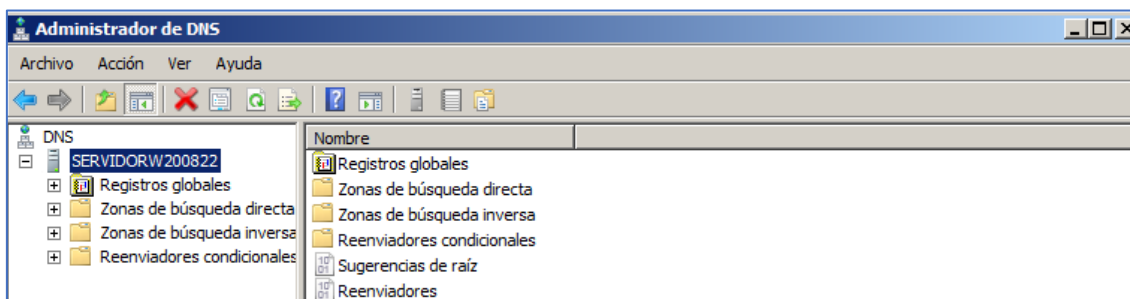
Ejecutamos el comando "netstat -a -n -p TCP" para obtener los puertos TCP a la escucha.

```
C:\Users\Administrador>netstat -a -n -p UDP | find "127.0.0.1:53"
UDP    127.0.0.1:53          *:*

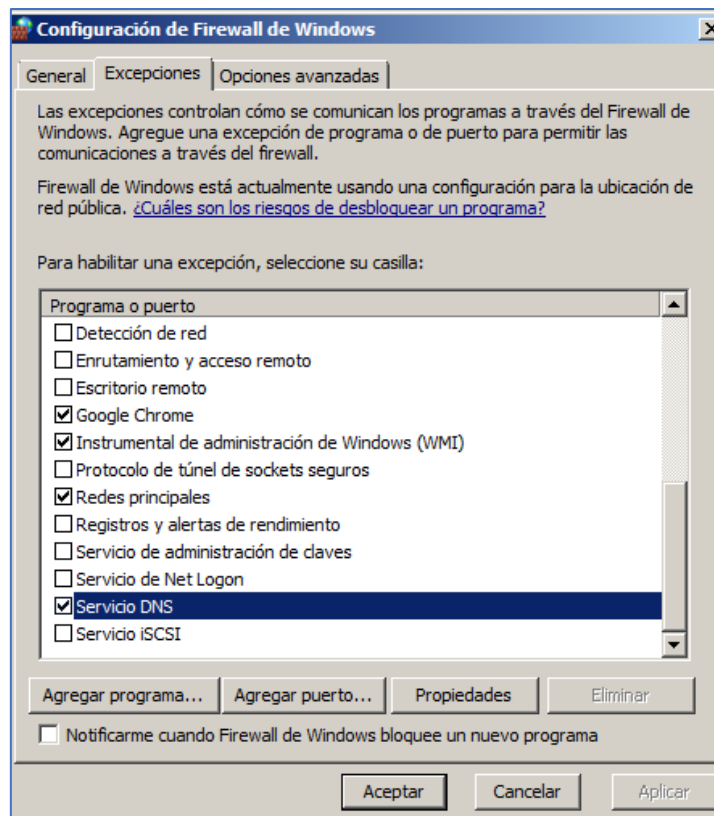
C:\Users\Administrador>_
```

Ejecutamos el comando "netsat -a -n -p UDP | find "1270.0.1:53" para obtener el puerto UDP a la esucha en la IP de Loopback del sistema.

Comprobamos que el puerto 53 está a la escucha en las IPs de Loopback y la asignada al sistema. El Puerto 53 es el usado por el servicio DNS por ser un puerto que en la mayoría de los casos está abierto en los sistemas para transmitir peticiones DNS. Generalmente el servicio DNS usa el protocolo UDP por su baja latencia, y un menor impacto en el uso de recursos de la red, pero en determinados casos en los que la petición pueda exceder los 512 bytes, se encargará de resolverla el protocolo TCP.



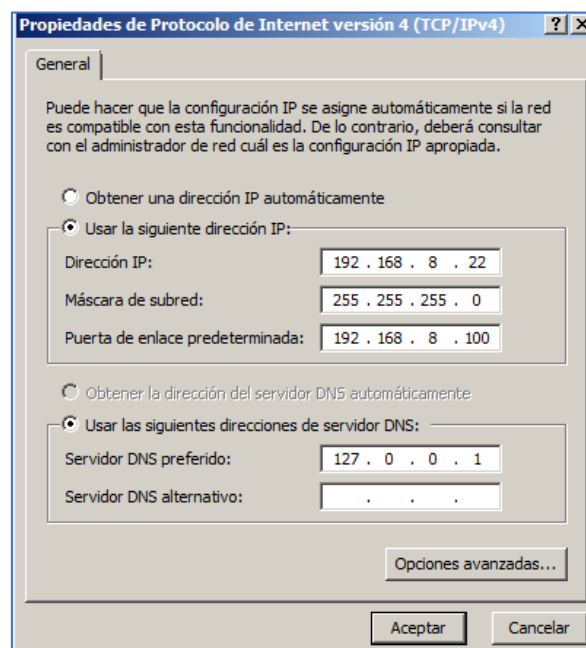
Accedemos al administrador DNS y vemos su contenido.



Comprobamos que el firewall de Windows ha creado una excepción para el servicio DNS.

2. Configuración del servidor como solo cache:

Para configurar el servidor como sólo cache y comprobar que el servidor resuelve consultas recursivas, vamos a configurar el protocolo IPv4 para que utilice el servidor DNS instalado en el sistema local.

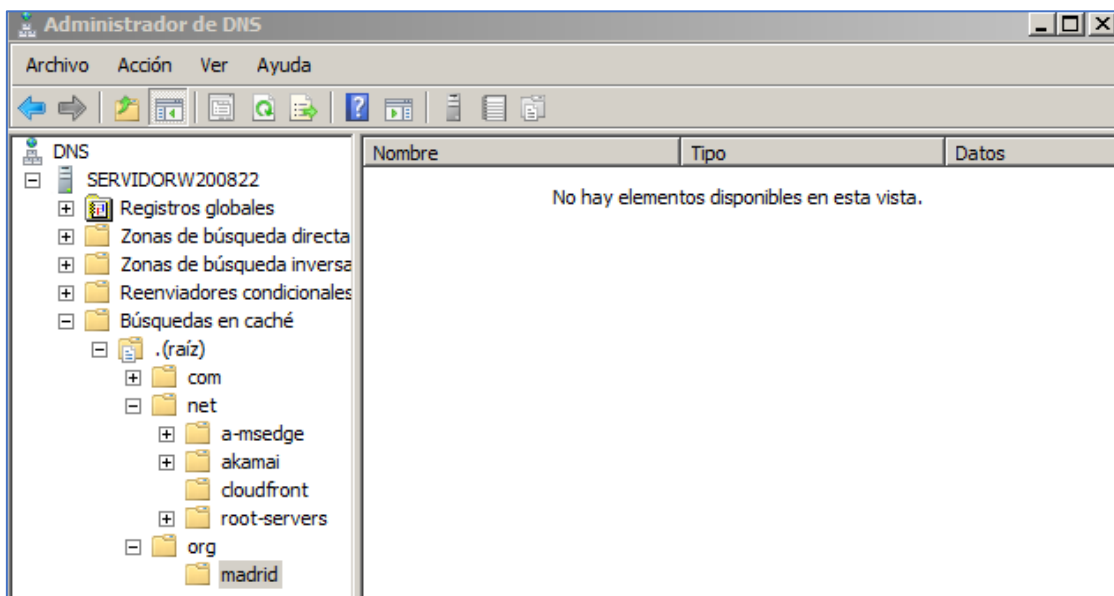


Configuración del protocolo IPv4 asignando el servidor DNS instalado "127.0.0.1".

```
C:\Users\Administrador>nslookup www.madrid.org
Servidor: localhost
Address: 127.0.0.1

Respuesta no autoritativa:
Nombre: d3omk6xn5p4d3d.cloudfront.net
Addresses: 2600:9000:20c8:d600:1a:83ee:1240:93a1
           2600:9000:20c8:4000:1a:83ee:1240:93a1
           2600:9000:20c8:8000:1a:83ee:1240:93a1
           2600:9000:20c8:3200:1a:83ee:1240:93a1
           2600:9000:20c8:6e00:1a:83ee:1240:93a1
           2600:9000:20c8:4800:1a:83ee:1240:93a1
           2600:9000:20c8:7200:1a:83ee:1240:93a1
           2600:9000:20c8:0:1a:83ee:1240:93a1
           54.192.106.24
           54.192.106.98
           54.192.106.51
           54.192.106.91
Alias(es): www.madrid.org
```

Comprobamos que el servidor DNS instalado en la máquina funciona correctamente.



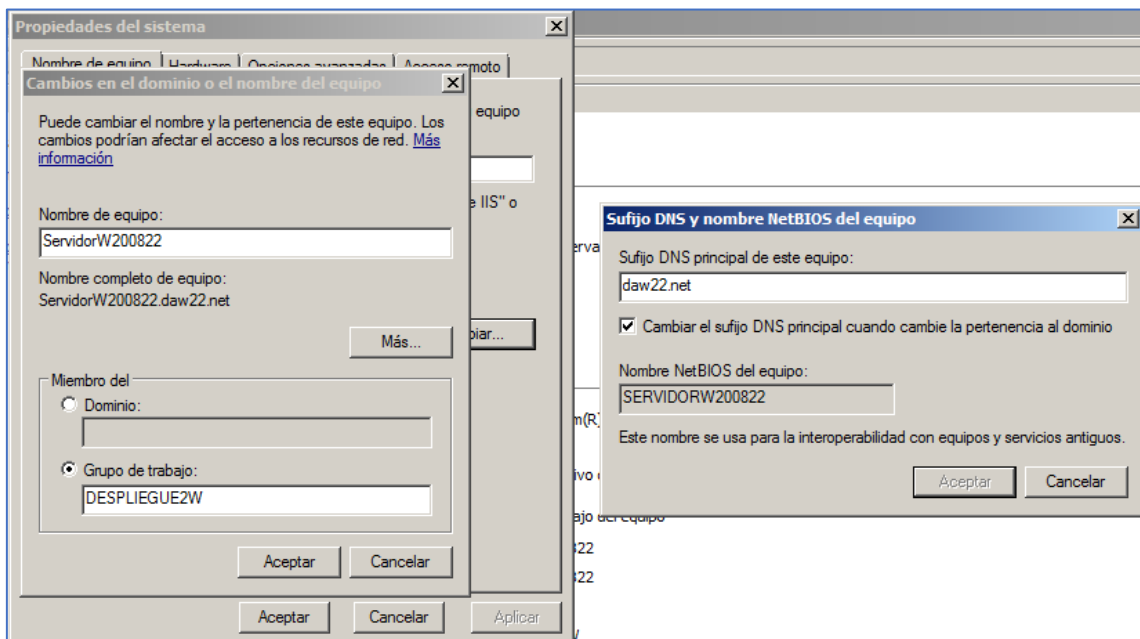
Activamos la vista avanzada en el administrado de DNS.

Comprobamos que se ha generado una serie carpetas, esto es debido a la resolución de consultas recursivas.

3.3 Servidor DNS en Microsoft Windows Server 2008. Configuración del servidor como primario (maestro) para una zona de resolución directa.

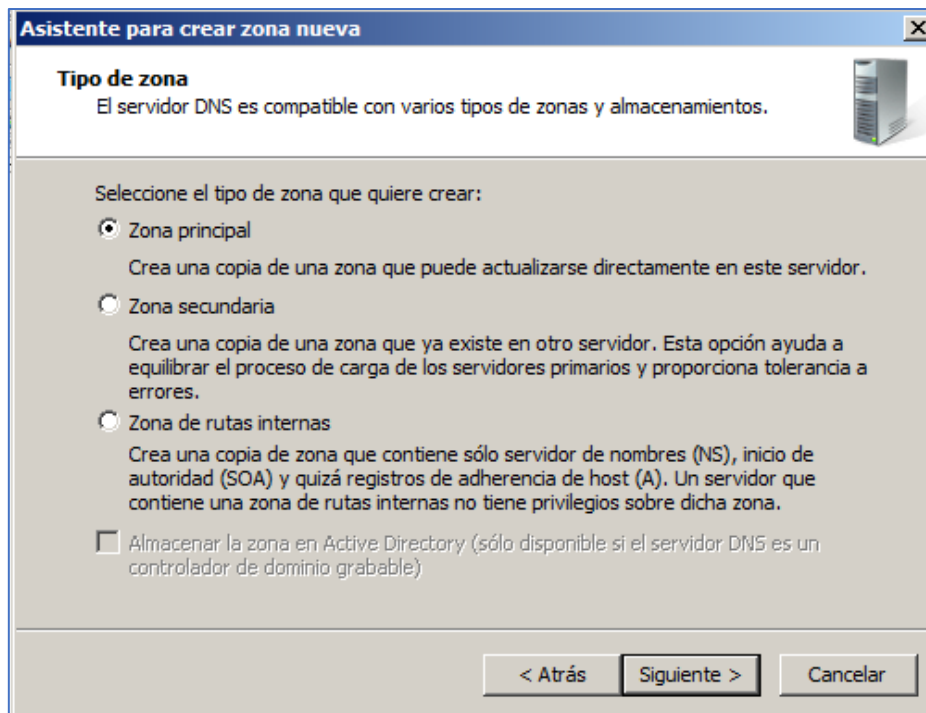
Configuración del sufijo DNS del equipo:

Para empezar, iremos a la configuración avanzada del sistema y cambiaremos el nombre del equipo.

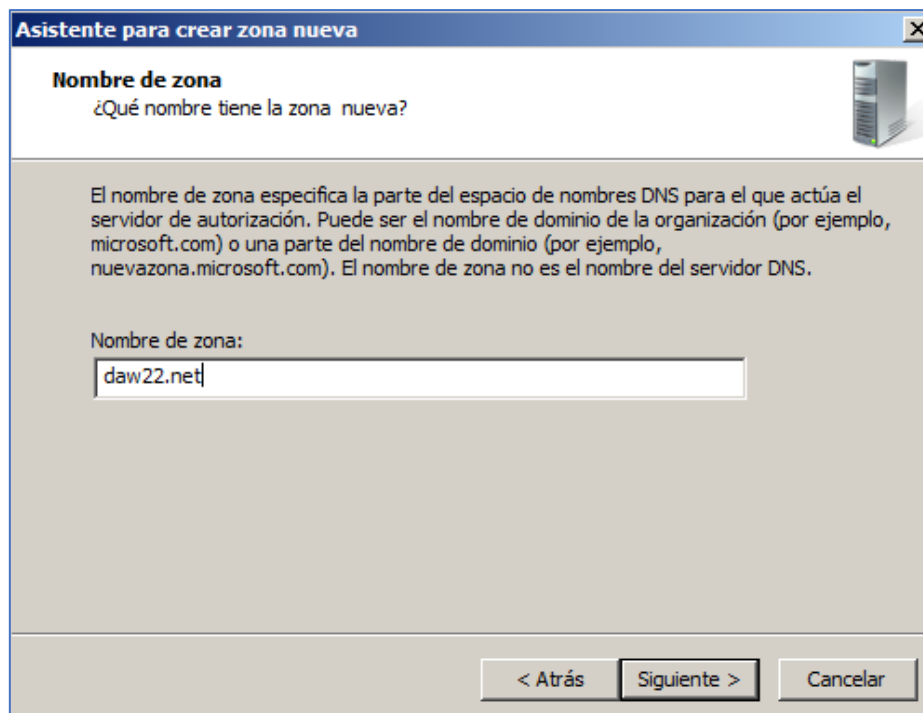


Cambio de nombre del sistema con el sufijo DNS "daw22.net".

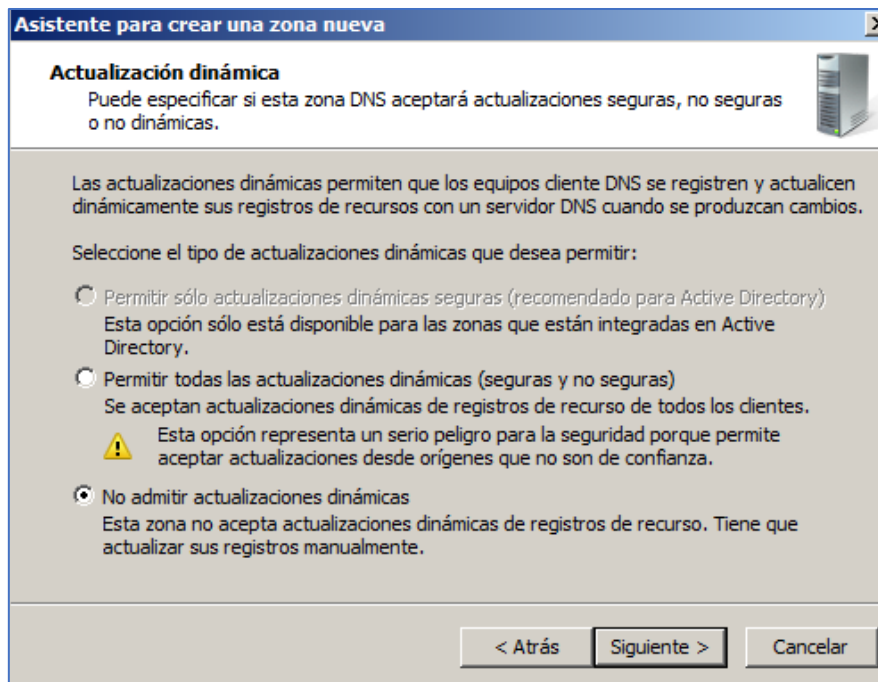
A continuación, crearemos una nueva zona de búsqueda directa, para ello accederemos al administrador de DNS y pincharemos con el botón derecho en Zonas de búsqueda directa y seleccionaremos nueva zona.



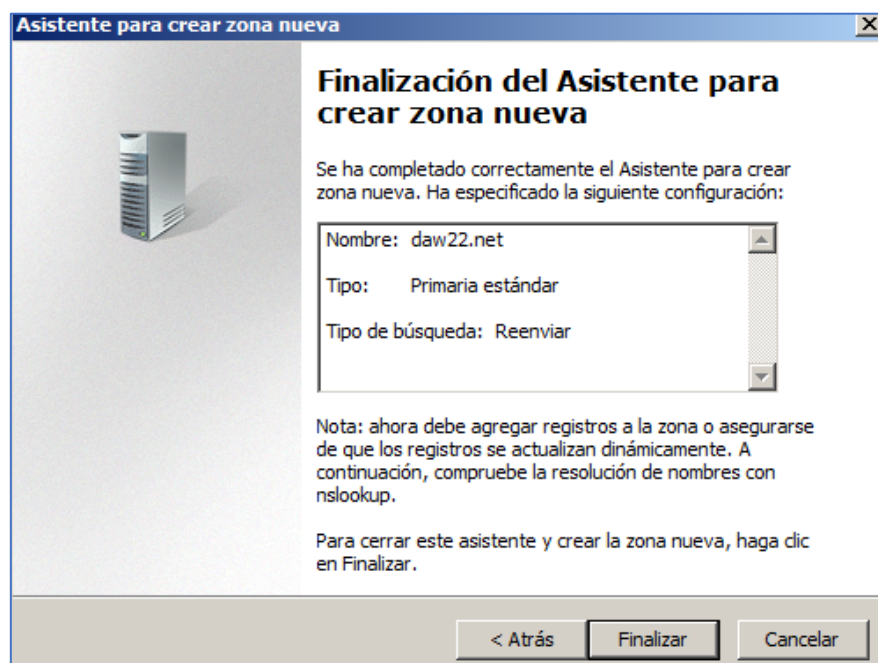
Seleccionamos el tipo de zona como principal.



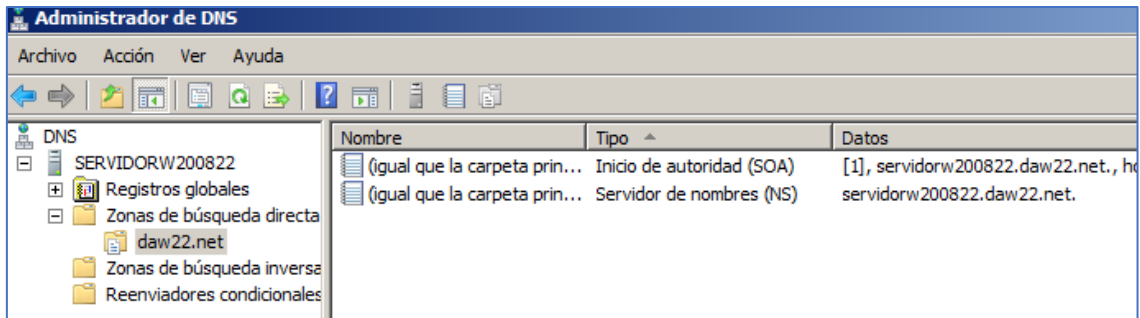
Asignamos el nombre de zona "daw22.net".



Seleccionamos "No admitir actualizaciones dinámicas".



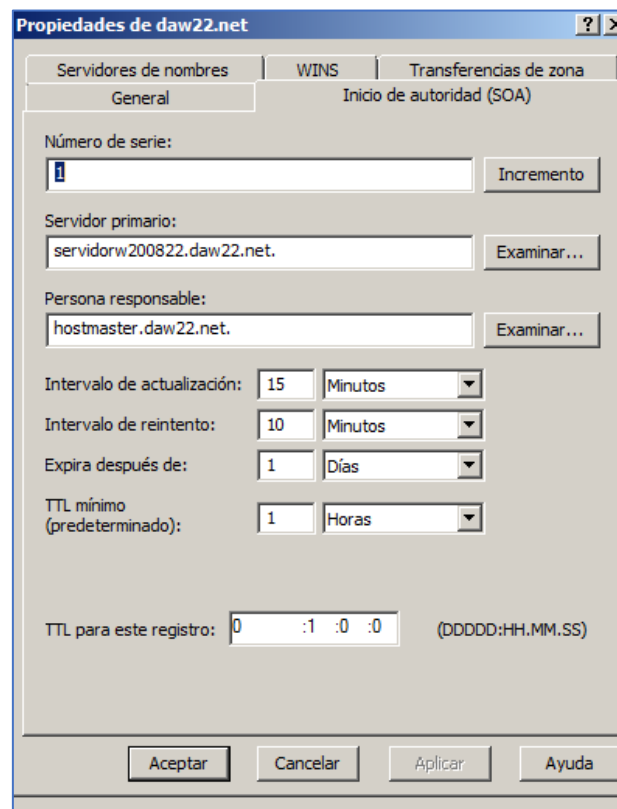
Configuración final de la nueva zona.



Observamos que se ha creado la zona correctamente y que han aparecido los registros de recursos SOA, y NS.

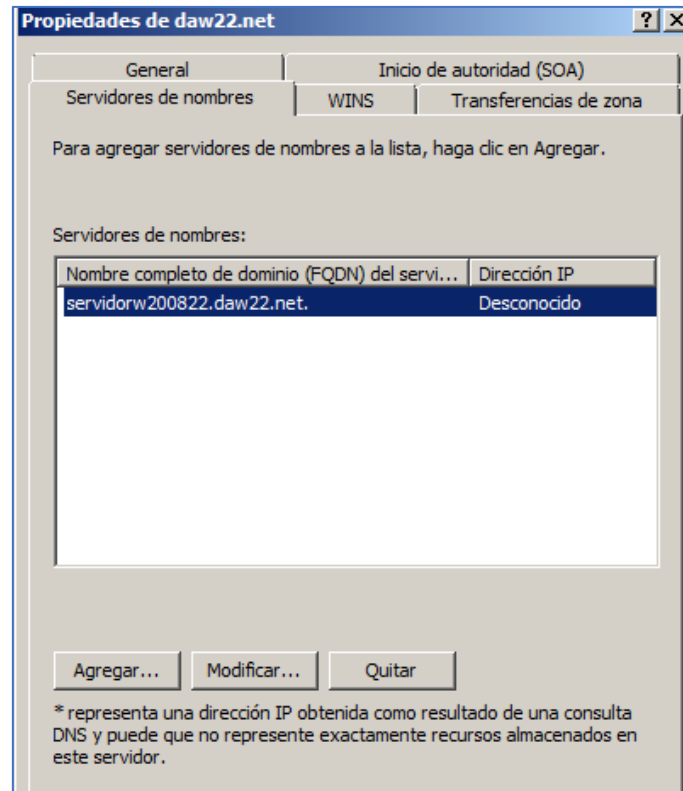
Estos indican que el servidor DNS para el dominio, es este equipo. El registro SOA (*Start of Authority*) contiene una serie de datos como:

- El nombre de dominio del servidor DNS primario de la zona.
- El nombre de dominio que indica el correo de la persona responsable de la zona.
- Un contador que incrementa con cada actualización de la zona.
- El intervalo de tiempo de actualización de la zona.
- El intervalo de tiempo de reintento de petición en caso de fallo.
- El límite máximo de tiempo hasta que la zona deje de ser autoritativa.
- El límite de tiempo de vida para exploraciones de la zona TTL (*Time To Live*).



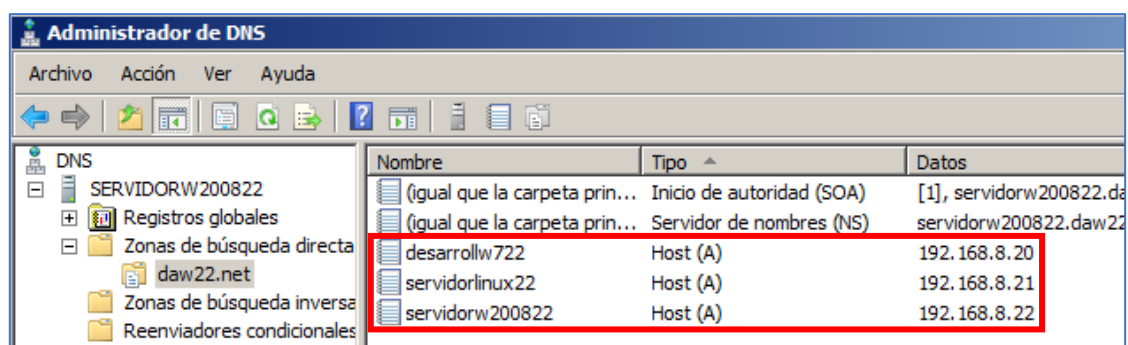
Configuración del registro SOA.

Por otra parte, el registro NS (Name Server) almacena los nombres completos o FQDN (Fully Qualified Domain Name) para un dominio.



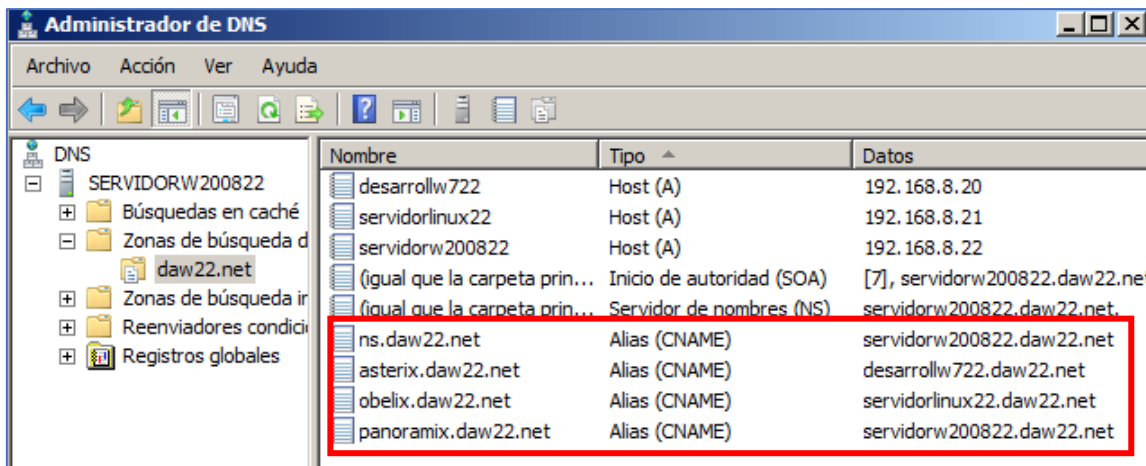
Configuración del registro NS.

A continuación, crearemos los registros A (Adress) de las máquinas virtuales con sus respectivas IP.



Registros A creados en la zona de búsqueda directa "daw22.net".

Seguidamente, crearemos los registros CNAME o alias de las máquinas.



Registros CNAME creados en la zona de búsqueda directa "daw22.net".

nslookup a Registros A

```
C:\Users\Administrador>nslookup desarrollw722
Servidor: localhost
Address: 127.0.0.1

Nombre: desarrollw722.daw22.net
Address: 192.168.8.20

C:\Users\Administrador>nslookup servidorlinux22
Servidor: localhost
Address: 127.0.0.1

Nombre: servidorlinux22.daw22.net
Address: 192.168.8.21

C:\Users\Administrador>nslookup servidorw200822
Servidor: localhost
Address: 127.0.0.1

Nombre: servidorw200822.daw22.net
Address: 192.168.8.22
```

Comprobamos que el servidor resuelve las consultas a los nombres de la zona "daw22.net" tanto con el sufijo DNS como sin él.

nslookup a Registros CNAME

```
C:\Users\Administrador>nslookup ns.daw22.net
Servidor: localhost
Address: 127.0.0.1

Nombre: servidorw200822.daw22.net
Address: 192.168.8.22
Aliases: ns.daw22.net.daw22.net

C:\Users\Administrador>nslookup asterix.daw22.net
Servidor: localhost
Address: 127.0.0.1

Nombre: desarrollw722.daw22.net
Address: 192.168.8.20
Aliases: asterix.daw22.net.daw22.net

C:\Users\Administrador>nslookup obelix.daw22.net
Servidor: localhost
Address: 127.0.0.1

Nombre: servidorlinux22.daw22.net
Address: 192.168.8.21
Aliases: obelix.daw22.net.daw22.net

C:\Users\Administrador>nslookup panoramix.daw22.net
Servidor: localhost
Address: 127.0.0.1

Nombre: servidorw200822.daw22.net
Address: 192.168.8.22
Aliases: panoramix.daw22.net.daw22.net
```

Comprobamos que el servidor resuelve consultas a los alias creados anteriormente.

A continuación comprobaremos la resolución inversa de las IP asociadas a los registros.

```
C:\Users\Administrador>nslookup 192.168.8.20
Servidor: localhost
Address: 127.0.0.1

*** localhost no se puede encontrar 192.168.8.20: Non-existent domain

C:\Users\Administrador>nslookup 192.168.8.21
Servidor: localhost
Address: 127.0.0.1

*** localhost no se puede encontrar 192.168.8.21: Non-existent domain

C:\Users\Administrador>nslookup 192.168.8.22
Servidor: localhost
Address: 127.0.0.1

*** localhost no se puede encontrar 192.168.8.22: Non-existent domain

C:\Users\Administrador>_
```

Comprobamos que no puede resolver la consulta.

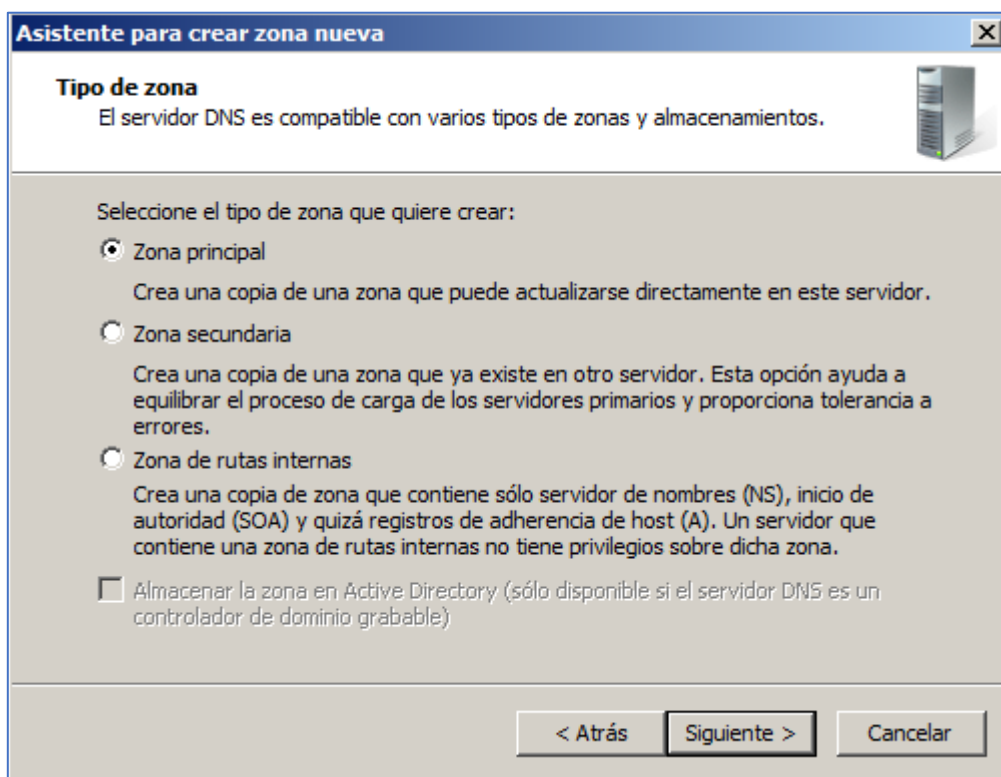
Esto es debido a que todavía no hemos configurado estos registros en la zona de búsqueda inversa.

3.4 Servidor DNS en Microsoft Windows Server 2008.

Configuración del servidor como primario (maestro) para una zona inversa.

Configuración de la zona de resolución inversa:

En primer lugar, crearemos una nueva zona de búsqueda inversa, para ello seguiremos los mismos pasos que en el caso anterior, pero esta vez en la pestaña "Zonas de búsqueda inversa".



Seleccionamos el tipo de zona como principal.

Asistente para nueva zona

Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Elija si desea crear una zona de búsqueda inversa para direcciones IPv4 o direcciones IPv6.

☒ Zona de búsqueda inversa para IPv4

☐ Zona de búsqueda inversa para IPv6

< Atrás Siguiendo > Cancelar

Seleccionamos la opción "Zona de búsqueda inversa para IPv4".

Asistente para crear zona nueva

Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Para identificar la zona de búsqueda inversa, escriba el Id. de red o el nombre de zona.

☒ Id. de red:

192.168.8

El Id de red es la parte de la dirección IP que pertenece a esta zona. Escriba el Id. de red en su orden normal (no en el inverso).

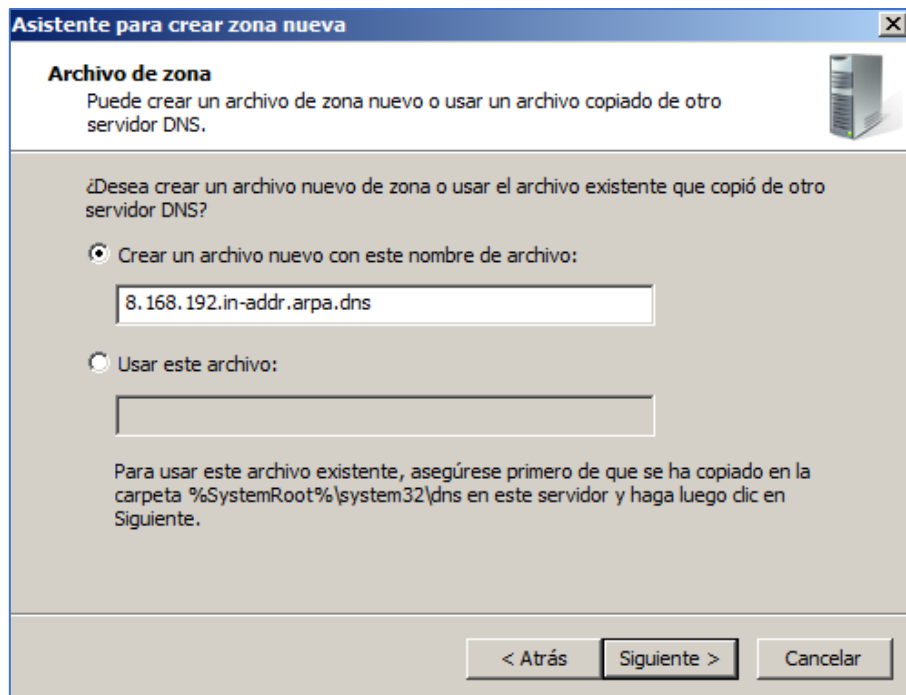
Si usa un cero en el Id de red, aparecerá en el nombre de la zona. Por ejemplo, el Id de red 10 crearía la zona 10.in-addr.arpa, y el Id de red 10.0 crearía la zona 0.10.in-addr.arpa.

☐ Nombre de la zona de búsqueda inversa:

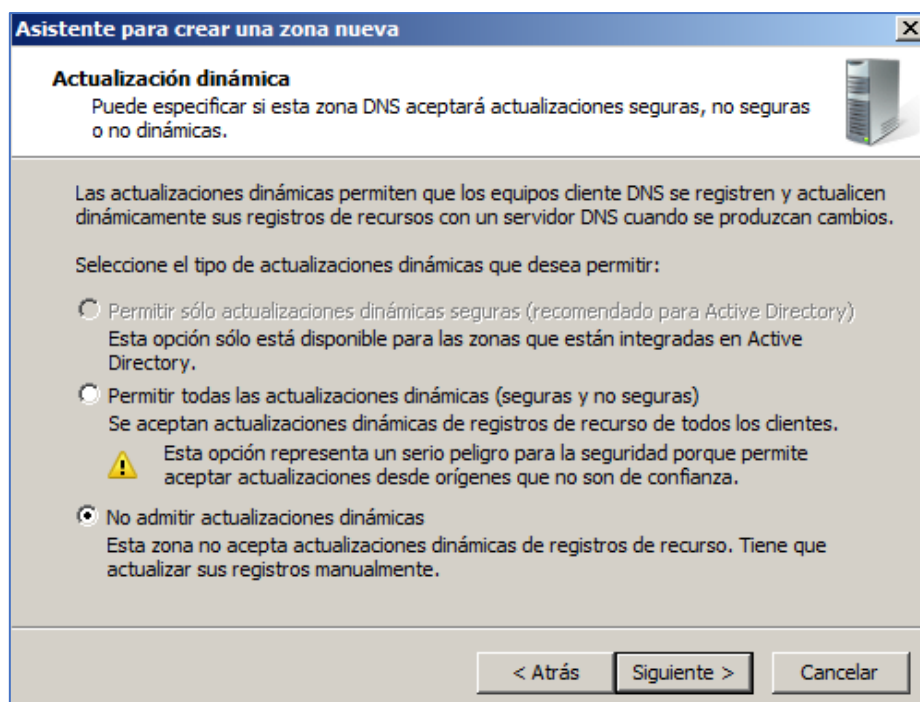
8.168.192.in-addr.arpa

< Atrás Siguiendo > Cancelar

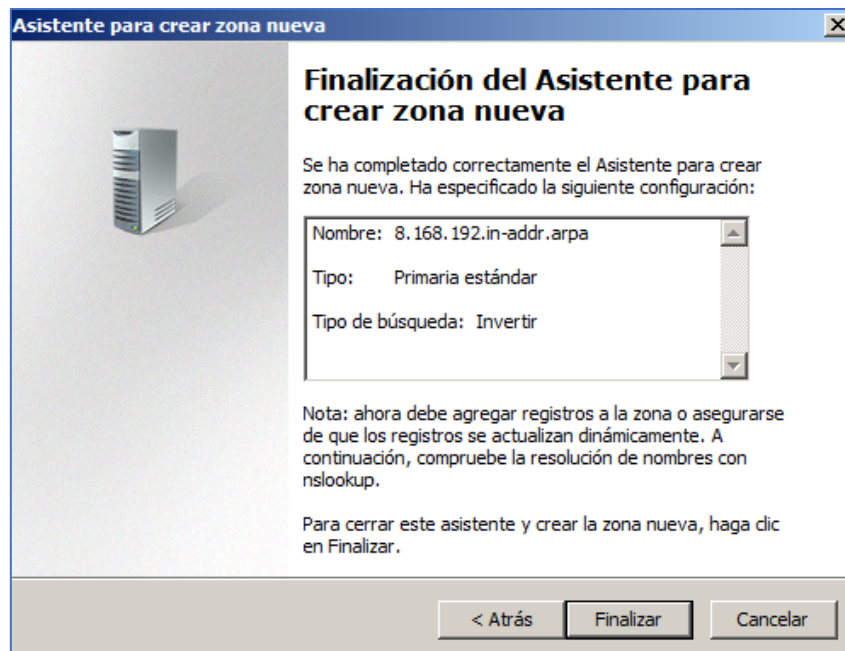
indicamos el Id. de red "192.168.8".



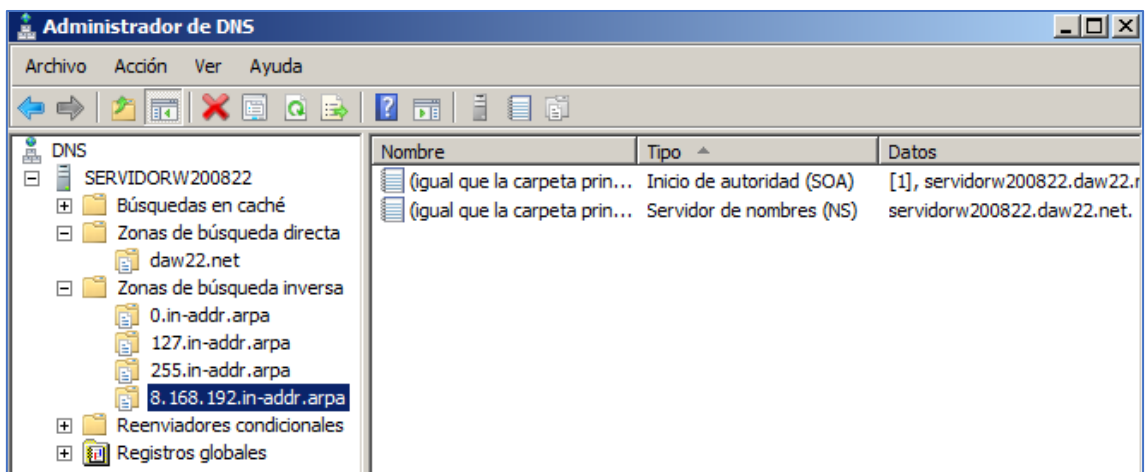
Seleccionamos la opción "Crear un archivo nuevo con este nombre de archivo". Y dejamos el nombre que pone por defecto.



Seleccionamos la opción "No admitir actualizaciones dinámicas".



Configuración final de la nueva zona de búsqueda inversa "8.168.192.in-addr.arpa".



Comprobamos que se ha creado correctamente la nueva zona y que se han añadido los registros SOA y NS indicando que el servidor DNS para el dominio es este equipo.

The screenshot shows the 'Propiedades de 8.168.192.in-addr.arpa' dialog box with the 'Inicio de autoridad (SOA)' tab selected. The 'General' sub-tab is also active. The fields are as follows:

- Número de serie: 1 (with an 'Incremento' button)
- Servidor primario: servidorw200822.daw22.net. (with an 'Examinar...' button)
- Persona responsable: hostmaster.daw22.net. (with an 'Examinar...' button)
- Intervalo de actualización: 15 Minutos
- Intervalo de reintento: 10 Minutos
- Expira después de: 1 Días
- TTL mínimo (predeterminado): 1 Horas
- TTL para este registro: 0 : 1 : 0 : 0 (DDDD:HH.MM.SS)

Buttons at the bottom: Aceptar, Cancelar, Aplicar, Ayuda.

Propiedades del registro SOA de la zona "8.168.192.in-addr.arpa".

Al igual que las propiedades del registro SOA de la zona de búsqueda directa creada anteriormente, observamos que tiene las mismas opciones de configuración.

The screenshot shows the 'Propiedades de 8.168.192.in-addr.arpa' dialog box with the 'Servidores de nombres' tab selected. The 'General' sub-tab is also active. The fields are as follows:

- Para agregar servidores de nombres a la lista, haga clic en Agregar.
- Servidores de nombres: A table with two columns: 'Nombre completo de dominio (FQDN) del servi...' and 'Dirección IP'. The first row contains 'servidorw200822.daw22.net.' and '[192.168.8.22*]'.
- Buttons: Agregar..., Modificar..., Quitar
- * representa una dirección IP obtenida como resultado de una consulta DNS y puede que no represente exactamente recursos almacenados en este servidor.

Buttons at the bottom: Aceptar, Cancelar, Aplicar, Ayuda.

Propiedades del registro NS de la zona "8.168.192.in-addr.arpa".

Observamos que aparece el registro A creado anteriormente con el nombre de dominio "servidorw200822.daw22.net" y con su IP asociada.

A continuación, crearemos los registros PTR o Puntero que apuntarán los otros registros pertenecientes a las máquinas de la red virtual, para haremos click derecho sobre la zona "8.168.192.in-addr.arpa" y seleccionaremos la opción "nuevo Puntero (PTR)".

Configuración del nuevo registro PTR que apunta a la máquina "desarrollw722.daw22.net".

Repetimos el proceso con el resto de hosts.

Nombre	Tipo	Datos
(igual que la carpeta prin...	Inicio de autoridad (SOA)	[1], servidorw200822.daw22.net.
(igual que la carpeta prin...	Servidor de nombres (NS)	servidorw200822.daw22.net.
192.168.8.20	Puntero (PTR)	desarrollw722.daw22.net
192.168.8.21	Puntero (PTR)	servidorlinux22.daw22.net
192.168.8.22	Puntero (PTR)	servidorw200822.daw22.net

Registros PTR creados para la resolución inversa de las IP asociadas a los hosts.

Comprobar la configuración:

```
C:\Users\Administrador>nslookup 192.168.8.20
Servidor: localhost
Address: 127.0.0.1

Nombre: desarrollw722.daw22.net
Address: 192.168.8.20

C:\Users\Administrador>nslookup 192.168.8.21
Servidor: localhost
Address: 127.0.0.1

Nombre: servidorlinux22.daw22.net
Address: 192.168.8.21

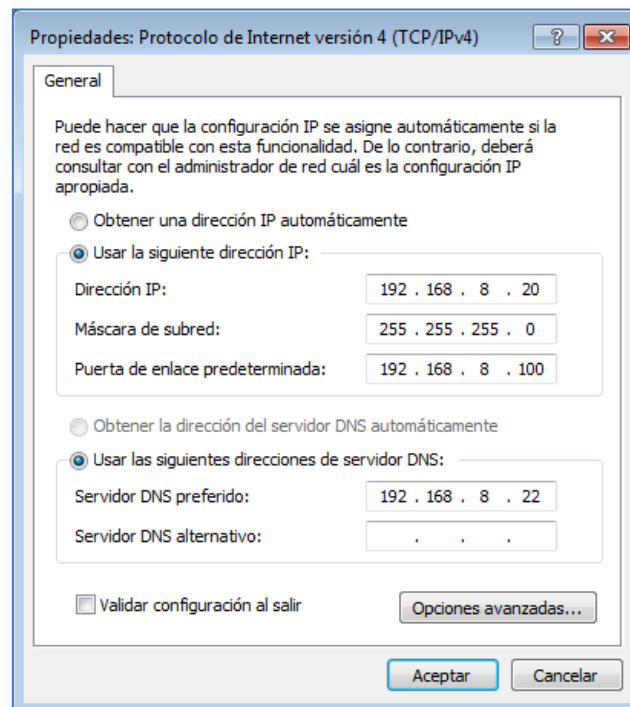
C:\Users\Administrador>nslookup 192.168.8.22
Servidor: localhost
Address: 127.0.0.1

Nombre: servidorw200822.daw22.net
Address: 192.168.8.22
```

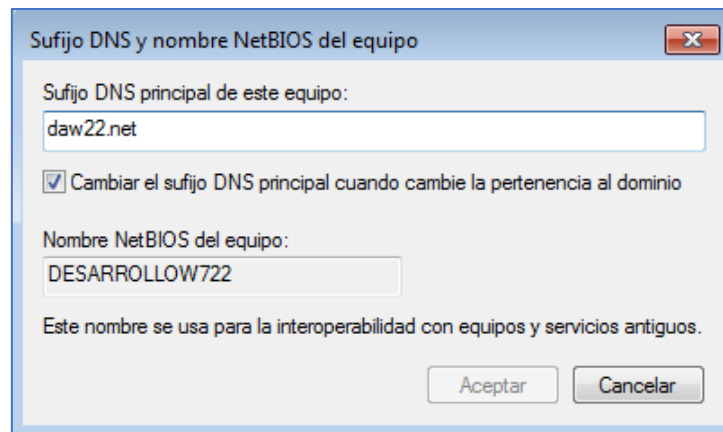
Comprobamos que ahora sí podemos hacer una resolución inversa indicando la IP y nos devuelve el nombre del host asociado.

3.8 Cliente DNS en las otras máquinas.

Configuración de la máquina desarrollw722.



Configuramos el protocolo TCP/IPv4 para que use el servidor DNS configurado.



Añadimos el sufijo DNS en la configuración avanzada del sistema.

```
C:\Users\alumno>nslookup servidorw200822.daw22.net
Servidor:  servidorw200822.daw22.net
Address:  192.168.8.22

Nombre:  servidorw200822.daw22.net
Address:  192.168.8.22

C:\Users\alumno>nslookup 192.168.8.22
Servidor:  servidorw200822.daw22.net
Address:  192.168.8.22

Nombre:  servidorw200822.daw22.net
Address:  192.168.8.22

C:\Users\alumno>_
```

Comprobamos que tanto la resolución directa como la inversa funcionan correctamente y la respuesta es autoritativa.

```
C:\Users\alumno>nslookup servidorw200822
Servidor:  servidorw200822.daw22.net
Address:  192.168.8.22

Nombre:  servidorw200822.daw22.net
Address:  192.168.8.22

C:\Users\alumno>_
```

Comprobamos que resuelve correctamente sin usar el sufijo DNS.

Configuración de la máquina ServidorLinux22:

```
#The loopback network interface
auto lo
iface lo inet loopback

#The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.8.21
    netmask 255.255.255.0
    gateway 192.168.8.100
    dns-nameservers 192.168.8.22
    dns-search daw22.net
```

Configuración del fichero “/etc/network/interfaces” con el servidor DNS configurado y el sufijo “daw22.net” especificado.

```
alumno@ServidorLinux21:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.8.22
search daw22.net
alumno@ServidorLinux21:~$
```

Comprobamos que la configuración se ha aplicado correctamente y la máquina usa el servidor DNS configurado.

```
alumno@ServidorLinux21:~$ cat /etc/hostname
ServidorLinux21.daw22.net
alumno@ServidorLinux21:~$
```

Configuración del fichero “/etc/hostname”.

```
127.0.0.1    localhost
127.0.1.1    ServidorLinux22.daw22.net

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

Configuración del fichero “etc/hosts”.

```

alumno@ServidorLinux21:~$ dig desarrollw722.daw22.net

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> desarrollw722.daw22.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2805
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;desarrollw722.daw22.net.      IN      A

;; ANSWER SECTION:
desarrollw722.daw22.net. 3600    IN      A      192.168.8.20

;; Query time: 1 msec
;; SERVER: 192.168.8.22#53(192.168.8.22)
;; WHEN: Sun Nov 15 17:22:20 CET 2020
;; MSG SIZE rcvd: 68

alumno@ServidorLinux21:~$

```

Comprobamos que responde el servidor "192.168.8.22" y nos devuelve la IP "192.168.8.20" asociada al nombre de la consulta que hemos realizado.

```

alumno@ServidorLinux21:~$ dig servidorlinux22.daw22.net

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> servidorlinux22.daw22.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48406
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;servidorlinux22.daw22.net.    IN      A

;; ANSWER SECTION:
servidorlinux22.daw22.net. 3600    IN      A      192.168.8.21

;; Query time: 1 msec
;; SERVER: 192.168.8.22#53(192.168.8.22)
;; WHEN: Sun Nov 15 18:25:04 CET 2020
;; MSG SIZE rcvd: 70

alumno@ServidorLinux21:~$ _

```

Comprobamos que resuelve la consulta correctamente y nos devuelve la IP "192.168.8.21" asociada al nombre de la consulta que hemos realizado.

```

alumno@ServidorLinux21:~$ dig servidorw200822.daw22.net

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> servidorw200822.daw22.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41642
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;servidorw200822.daw22.net.      IN      A

;; ANSWER SECTION:
servidorw200822.daw22.net. 3600 IN      A      192.168.8.22

;; Query time: 1 msec
;; SERVER: 192.168.8.22#53(192.168.8.22)
;; WHEN: Sun Nov 15 18:27:57 CET 2020
;; MSG SIZE rcvd: 70

alumno@ServidorLinux21:~$ _

```

Comprobamos que resuelve la consulta correctamente y nos devuelve la IP "192.168.8.22" asociada al nombre de la consulta realizada.

```

alumno@ServidorLinux21:~$ dig -x 192.168.8.20

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> -x 192.168.8.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48921
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;20.8.168.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
20.8.168.192.in-addr.arpa. 3600 IN      PTR      desarrollw722.daw22.net.

;; Query time: 2 msec
;; SERVER: 192.168.8.22#53(192.168.8.22)
;; WHEN: Sun Nov 15 17:28:05 CET 2020
;; MSG SIZE rcvd: 91

alumno@ServidorLinux21:~$

```

Comprobamos que responde a la resolución inversa y nos devuelve el nombre "desarrollw722.daw.net" asociado a la IP "192.168.8.20".

```

alumno@ServidorLinux21:~$ dig -x 192.168.8.21

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> -x 192.168.8.21
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 16071
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 1280
;; QUESTION SECTION:
;21.8.168.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
21.8.168.192.in-addr.arpa. 3600 IN      PTR      servidorlinux22.daw22.net.

;; Query time: 1 msec
;; SERVER: 192.168.8.22#53(192.168.8.22)
;; WHEN: Sun Nov 15 18:34:22 CET 2020
;; MSG SIZE rcvd: 93

alumno@ServidorLinux21:~$

```

Comprobamos que responde a la resolución inversa y nos devuelve el nombre "servidorlinux22.daw22.net" asociado a la IP "192.168.8.21".

```

alumno@ServidorLinux21:~$ dig -x 192.168.8.22

; <<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> -x 192.168.8.22
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 55147
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 1280
;; QUESTION SECTION:
;22.8.168.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
22.8.168.192.in-addr.arpa. 3600 IN      PTR      servidorw200822.daw22.net.

;; Query time: 1 msec
;; SERVER: 192.168.8.22#53(192.168.8.22)
;; WHEN: Sun Nov 15 18:35:11 CET 2020
;; MSG SIZE rcvd: 93

alumno@ServidorLinux21:~$

```

Comprobamos que responde a la resolución inversa y nos devuelve el nombre "servidorw200822.daw22.net" asociado a la IP "192.168.8.22".

Con esta última configuración terminamos con la instalación del servicio DNS en las máquinas virtuales.