

Configuración Servicio DNS en Windows 2012 Server r2

1. Objetivos

En esta práctica aprenderás a instalar y configurar un servidor DNS. La primera parte consiste en una configuración básica donde se indica cómo realizar la configuración de resolución directa e inversa.

Posteriormente y una vez configurado el servidor DNS en Centos para ser el servidor DNS secundario, haremos una configuración de servidor secundario sobre el principal con el segundo servidor DNS. Después se realiza una configuración para gestionar subdominios donde el subdominio en cuestión se ha de gestionar con el segundo servidor DNS.

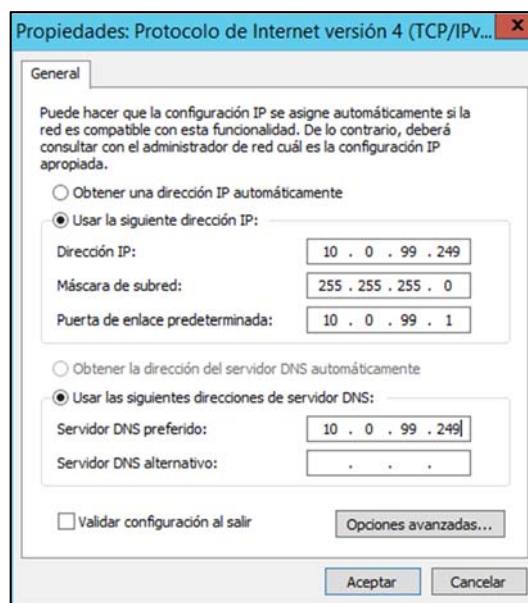
Finalmente aprenderemos como realizar labores de resolución de incidencias consultando los registros que genera el servicio.

La organización de esta práctica se resume en los siguientes pasos:

1. Instalación del Server 2012 r2
2. Configuración del servidor Cache con reenviadores
3. Configuración del Servidor DNS como Principal
4. Configuración del Servidor Secundario en Centos 7
5. Configuración para el funcionamiento con dos servidores DNS: principal (Windows 2012 server) y secundario (Centos 7)
6. Configurar un servidor Windows 2012 r2 como secundario, siendo servidor Centos Principal

2. Instalación del Server 2012 r2

Use la instantánea tomada en la configuración básica o proceda según lo indicado en la Práctica 1. Cambie el nombre del servidor a dnsW.grupoXX.net. Y coloque en la configuración de la tarjeta de la VLAN de producción como servidor DNS preferido la IP del propio servidor, 10.X.99.249

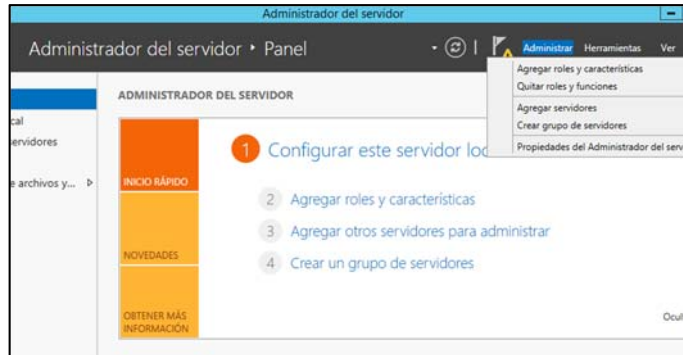


Paso 1. Instalación de la máquina cliente Windows 8.1

Use la instantánea tomada en la configuración básica o proceda según lo indicado en la Práctica 1.

Paso 2. Instalación servicio DNS

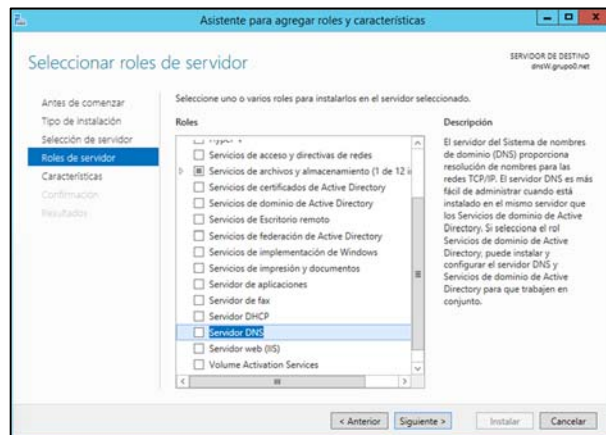
Una vez configuradas las tarjetas de red, hemos de instalar el servicio DNS:



Para ello, Administrar → Agregar roles y características.

Pulsamos en siguiente y seleccionamos “Instalación basada en características o en roles”.

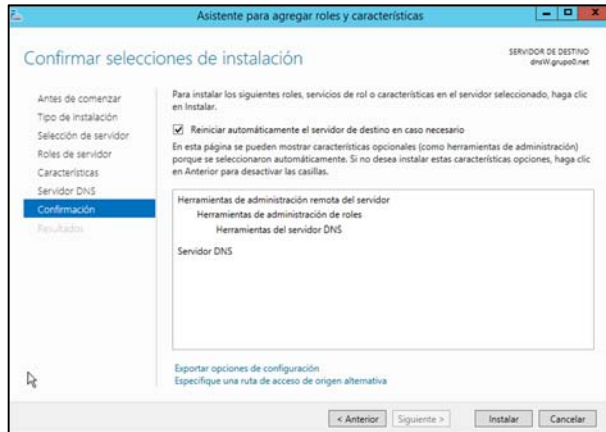
Pulsamos en siguiente, donde tendremos seleccionado nuestro servidor, volvemos a pulsar siguiente. Donde agregaremos el rol → Servidor DNS



Al seleccionarlo nos abre una ventana de diálogo, hacemos clic en Agregar Características.

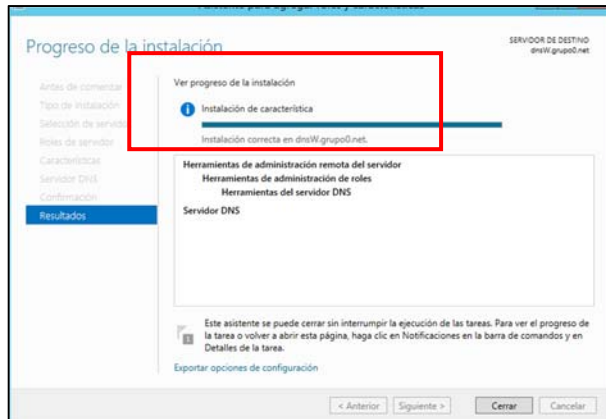
Clic en siguiente, donde nos permite añadir características, en nuestro caso no añadimos ninguna.

Damos clic en siguiente, otra vez a siguiente, donde nos pide confirmación. En esta pantalla seleccionamos “Reiniciar automáticamente el servidor de destino en caso necesario”.



Clic en instalar,

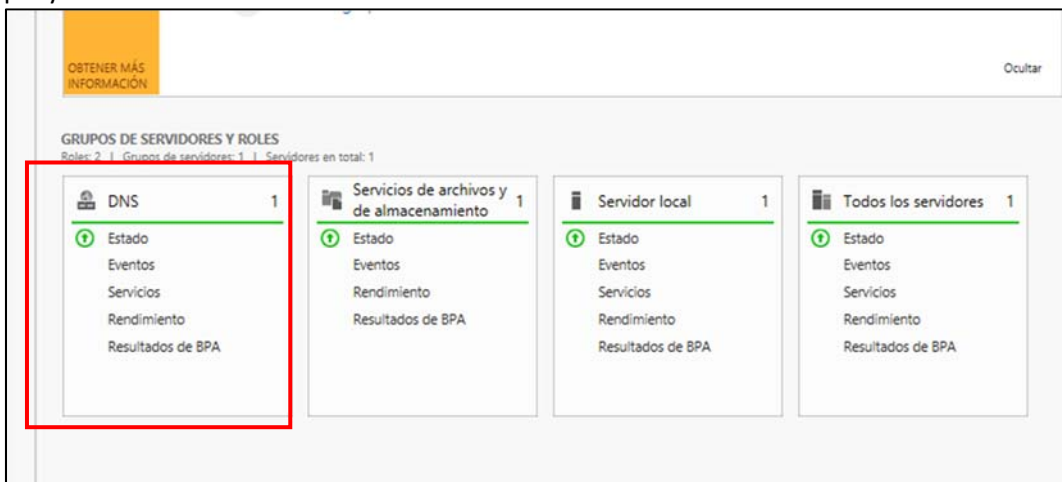
Una vez finalizada la instalación en la pantalla nos indicará si la instalación ha sido o no realizada de manera correcta.



Clic en cerrar, vemos no se ha reiniciado, al no ser necesario.

Si vamos al Panel del Administrador de servidor, haciendo doble clic en la tecla Inicio → Herramientas Administrativas, Administrador del servidor.

Vemos que ya tenemos DNS activado:



Otra comprobación que podemos hacer es consultar cuales son los puertos que el servidor gestiona, con el comando `netstat -a`. El puerto que utiliza el DNS es el 53: (dar a Control+C se pare, moverse con el cursor de la ventana al principio).



```
PS C:\Users\Administrador> netstat -a
Conexiones activas
Proto Dirección local Dirección remota Estado
TCP 0.0.0.0:135 dnsW:0 LISTENING
TCP 0.0.0.0:445 dnsW:0 LISTENING
TCP 0.0.0.0:5985 dnsW:0 LISTENING
TCP 0.0.0.0:47001 dnsW:0 LISTENING
TCP 0.0.0.0:49152 dnsW:0 LISTENING
TCP 0.0.0.0:49153 dnsW:0 LISTENING
TCP 0.0.0.0:49154 dnsW:0 LISTENING
TCP 0.0.0.0:49155 dnsW:0 LISTENING
TCP 0.0.0.0:49156 dnsW:0 LISTENING
TCP 0.0.0.0:49157 dnsW:0 LISTENING
TCP 0.0.0.0:49169 dnsW:0 LISTENING
TCP 10.0.99.249:53 dnsW:0 LISTENING
TCP 10.0.99.249:139 dnsW:0 LISTENING
TCP 10.0.100.249:53 dnsW:0 LISTENING
TCP 10.0.100.249:139 dnsW:0 LISTENING
```

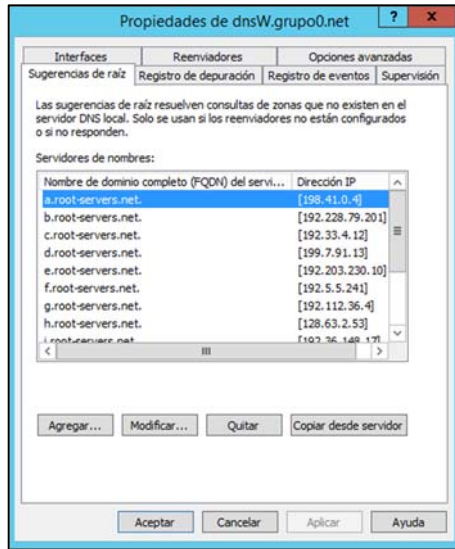
En el mismo comando se puede indicar que relacione la aplicación que está gestionando cada puerto `netstat -boa`

```
PS C:\Users\Administrador> netstat -boa
Conexiones activas
Proto Dirección local Dirección remota Estado PID
TCP 0.0.0.0:135 dnsW:0 LISTENING 524
RpcSs
[svchost.exe]
TCP 0.0.0.0:445 dnsW:0 LISTENING 4
No se puede obtener información de propiedad
TCP 0.0.0.0:5985 dnsW:0 LISTENING 4
No se puede obtener información de propiedad
TCP 0.0.0.0:47001 dnsW:0 LISTENING 4
No se puede obtener información de propiedad
TCP 0.0.0.0:49152 dnsW:0 LISTENING 344
[wininit.exe]
TCP 0.0.0.0:49153 dnsW:0 LISTENING 640
Eventlog
[svchost.exe]
TCP 0.0.0.0:49154 dnsW:0 LISTENING 440
[lsass.exe]
TCP 0.0.0.0:49155 dnsW:0 LISTENING 692
Schedule
[svchost.exe]
TCP 0.0.0.0:49156 dnsW:0 LISTENING 704
[spoolsv.exe]
TCP 0.0.0.0:49157 dnsW:0 LISTENING 432
No se puede obtener información de propiedad
TCP 0.0.0.0:49169 dnsW:0 LISTENING 2160
[dns.exe]
TCP 10.0.99.249:53 dnsW:0 LISTENING 2160
[dns.exe]
TCP 10.0.99.249:139 dnsW:0 LISTENING 4
No se puede obtener información de propiedad
TCP 10.0.100.249:53 dnsW:0 LISTENING 2160
[dns.exe]
TCP 10.0.100.249:139 dnsW:0 LISTENING 4
```

Podemos comprobar da servicio DNS, vamos a la ventana Shell y hacemos ping ping `www.google.es`, por ejemplo.

```
PS C:\Users\Administrador> ping www.google.es
Haciendo ping a www.google.es [74.125.206.94] con 32 bytes de datos:
Respuesta desde 74.125.206.94: bytes=32 tiempo=33ms TTL=45
Respuesta desde 74.125.206.94: bytes=32 tiempo=33ms TTL=45
Respuesta desde 74.125.206.94: bytes=32 tiempo=33ms TTL=45
Respuesta desde 74.125.206.94: bytes=32 tiempo=33ms TTL=45
Estadísticas de ping para 74.125.206.94:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 33ms, Máximo = 33ms, Media = 33ms
PS C:\Users\Administrador> _
```

En estos momentos no hemos definido ningún dominio y el servidor funciona como un servidor cache. Es decir, las consultas que se realizan sobre el servidor son resueltas mediante los servidores raíz (*roots*).



Para llegar a la figura de arriba. Dos caminos en el Panel: Herramientas→DNS→Acción→Propiedades.

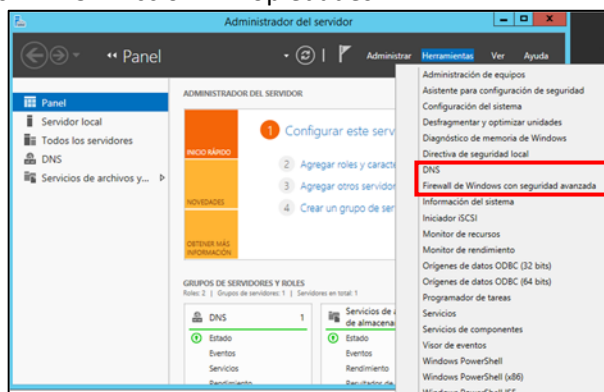
3. Configuración del servidor Cache con reenviadores

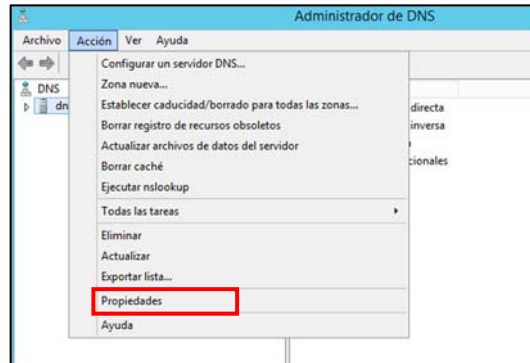
Tal como se ha indicado por defecto, las consultas se hacen a los servidores raíz sugeridos. Por lo que en ese caso, no es necesario configurar ningún servidor reenviador. Pero existe un modo de configuración en el cual configuramos servidores denominados reenviadores.

Cuando hacemos esto, nuestro servidor delega en estos servidores la resolución. Serán pues los servidores reenviadores los que consulten a otros servidores DNS. Habitualmente, como servidores reenviadores se utilizan los que facilita el Proveedor de la Conexión a Internet. Este tipo de configuración se usa para optimizar las consultas DNS dentro de una red local.

Para configurarla,

Panel →Herramientas→DNS→Acción→Propiedades





(Recuerde para llegar al Panel, si es necesario) Doble clic Inicio→Herramientas Administrativas→Administrador del servidor (donde llegamos al Panel).

Nos aparece la ventana de propiedades y seleccionamos la pestaña Reenviadores.

Clic en editar

Añadimos las direcciones de los servidores DNS de la UPV: 158.42.250.65, 158.42.250.195

Tras la validación tendremos configurados los servidores de reenvío.

Para probar el funcionamiento. Usaremos la orden nslookup y preguntamos por www.google.com

Si indicamos además la opción set debug, el comando facilita más información sobre cada consulta.

```

PS C:\Users\Administrador> nslookup
Servidor predeterminado: UnKnown
Address: 192.168.2.249

> set debug
> www.google.com
Servidor: UnKnown
Address: 192.168.2.249

-----
Got answer:
HEADER:
opcode = QUERY, id = 2, rcode = NXDOMAIN
header flags: response, want recursion, recursion avail.
questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:
www.google.com.grupo0.net, type = A, class = IN
AUTHORITY RECORDS:
-> net
ttl = 900 (15 mins)
primary name server = a.gtld-servers.net
responsible mail addr = nstld.verisign-grs.com
serial = 1468515479
refresh = 1800 (30 mins)
retry = 900 (15 mins)
expire = 604800 (7 days)
default TTL = 86400 (1 day)

-----
Got answer:
HEADER:
opcode = QUERY, id = 3, rcode = NXDOMAIN
header flags: response, want recursion, recursion avail.
questions = 1, answers = 0, authority records = 1, additional = 0

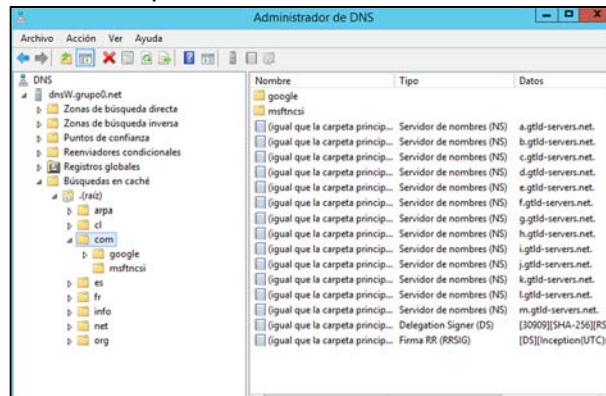
QUESTIONS:
www.google.com.grupo0.net, type = AAAA, class = IN
AUTHORITY RECORDS:
-> net
ttl = 900 (15 mins)
primary name server = a.gtld-servers.net
responsible mail addr = nstld.verisign-grs.com
serial = 1468515479
refresh = 1800 (30 mins)
retry = 900 (15 mins)
expire = 604800 (7 days)
default TTL = 86400 (1 day)

```

En el servidor, en el menú del Administrador DNS, podrás activar la opción avanzada que nos permite acceder a las opciones de la caché. Para activar, clic en Ver→Avanzada.



Aparece una nueva carpeta a la izquierda “Búsquedas de caché:”, donde se pueden ver los registros almacenados en la memoria caché. Estos registros son generados a medida que los clientes consultan las direcciones y el servidor las va resolviendo.



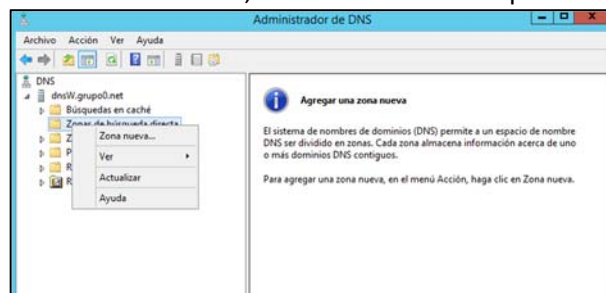
4. Configuración del Servidor DNS como Principal

En este punto vamos a configurar el servidor DNSW como servidor principal del dominio grupoXX.net.

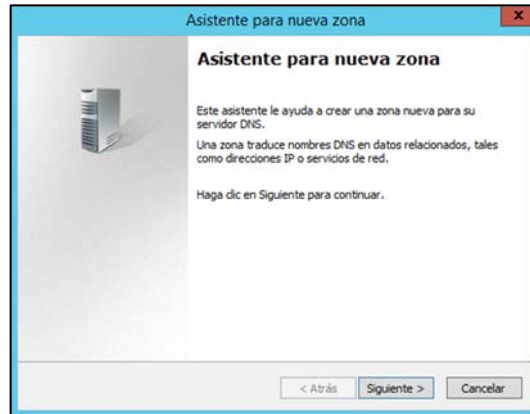
Antes de empezar desactivar la opción de usar reenviadores. Para ello eliminar los servidores de reenvío.

Procedamos,

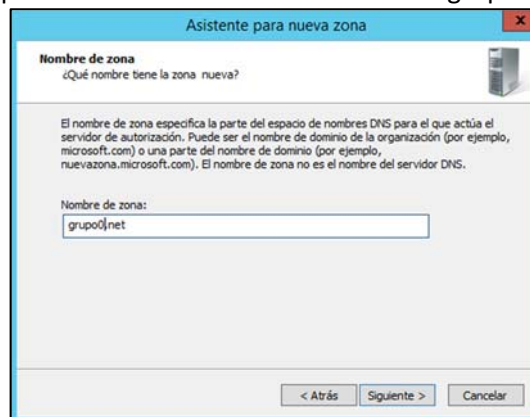
Hacer clic, con el botón derecho del ratón, sobre “Zonas de búsqueda directa”



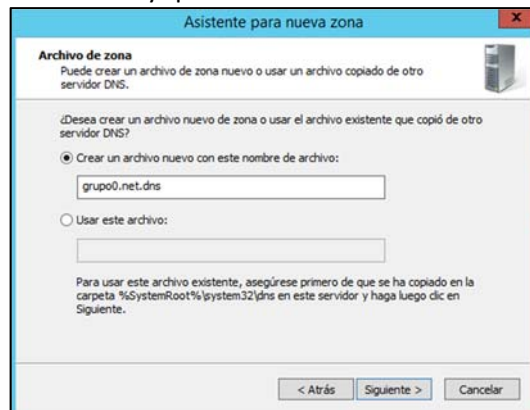
Seleccionamos Zona Nueva..., nos abrirá el asistente para crear una zona nueva que ha de gestionar el servidor DNS



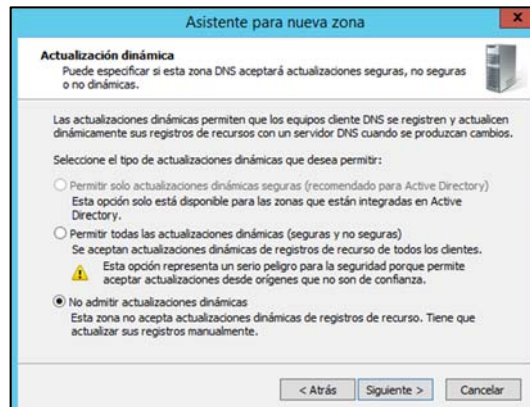
Seleccionamos Zona Principal, y damos a siguiente. A continuación el asistente nos pide el nombre a la nueva zona para tenerlo identificado. Colocamos grupoXX.net



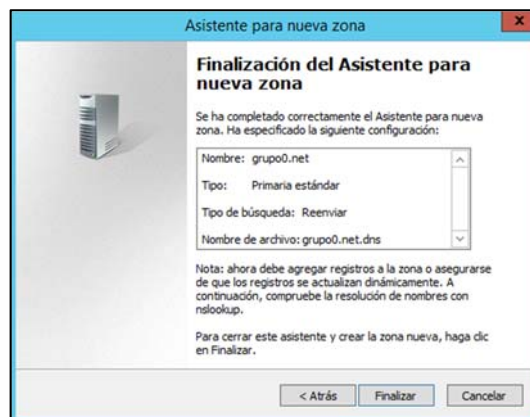
Seguidamente, el asistente consulta si la configuración de la nueva zona que se ha de crear se obtiene de un fichero ya creado o hay que crear uno nuevo.



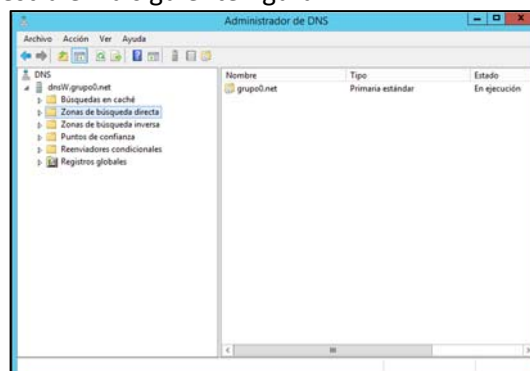
Siguiente, y seleccionamos la opción de “No admitir actualizaciones automáticas”.



Después de estos pasos se pide confirmación para crear la nueva zona con la configuración proporcionada.

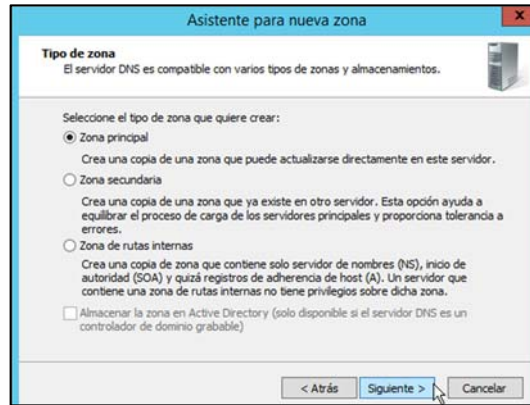


Como observarás, el nuevo dominio aparece como un elemento de la “Zona de búsqueda directa”, tal como se muestra en la siguiente figura.

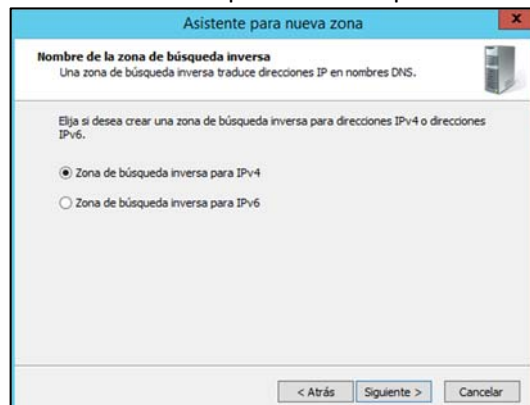


El siguiente paso es configurar la zona inversa. Para realizar este paso, en el Administrador de DNS, en la zona denominada “Zonas de búsqueda inversa, agregamos una nueva zona:

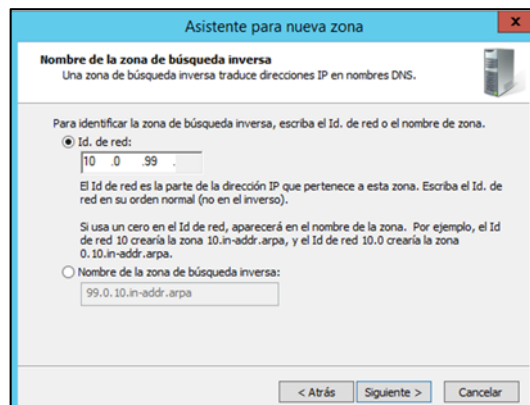
Avanzamos por el asistente. Seleccionamos como zona, Zona Principal:



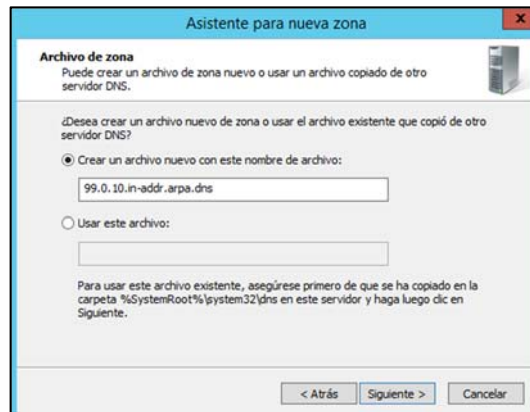
A continuación seleccionamos Zona de búsqueda inversa para IPv4:



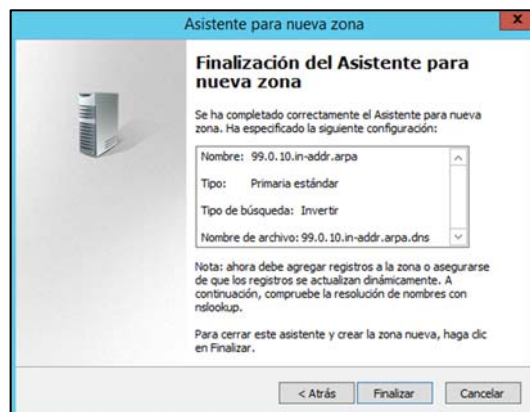
A continuación, el asistente solicita que se indique el tipo de red con el identificador. Indicaremos que se trata de una red del tipo 10.XX.99.0, tal como se observa en la siguiente figura.



El asistente consulta si se quiere crear un fichero nuevo o usar uno ya existente. Seleccionamos "Crear in archivo nuevo..."

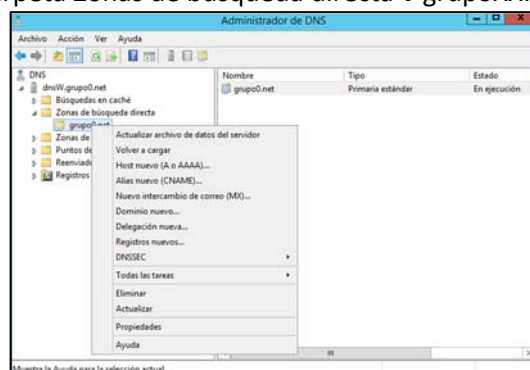


Clic en siguiente he indicamos que No admita actualizaciones automáticas. Finalmente el asistente nos pide confirmación para crear la zona inversa.



El paso siguiente es añadir registros en las zonas creadas.

Administrador DNS → Carpeta Zonas de búsqueda directa → grupoXX.net, botón derecho.



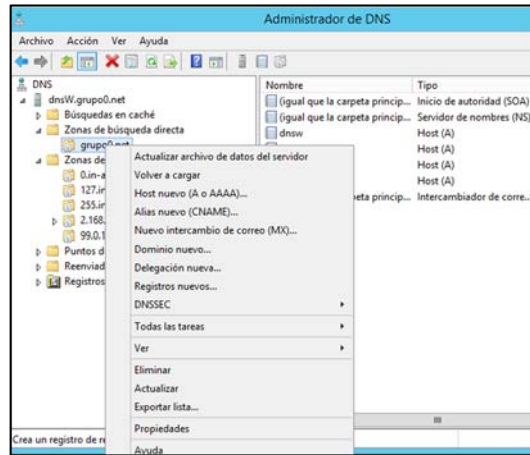
Aparecen una serie de opciones: tenemos que seleccionar la opción "Host Nuevo (A o AAAA)... para poder crear un registro nuevo.

Tras seleccionar la opción, aparece un formulario que permite agregar un registro nuevo de búsqueda directa a la zona. Rellenamos el formulario con el nombre de la máquina (dnsW) y su dirección IP (10.X.99.249). También es recomendable marcar la opción "Crear registro del puntero (PTR) asociado", ya que de esta manera, automáticamente se creará el registro inverso. Si no lo activamos deberíamos hacerlo de forma manual.

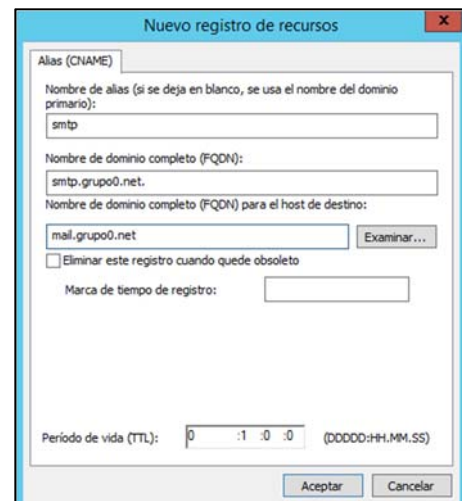
Aprovecharemos para crear uno para el servidor secundario, recordad que usaremos Centos 7, como Sistema Operativo. Lo llamaremos dnsc.

Y otro equipo denominado *mail*, con la dirección 10.XX.99.230.

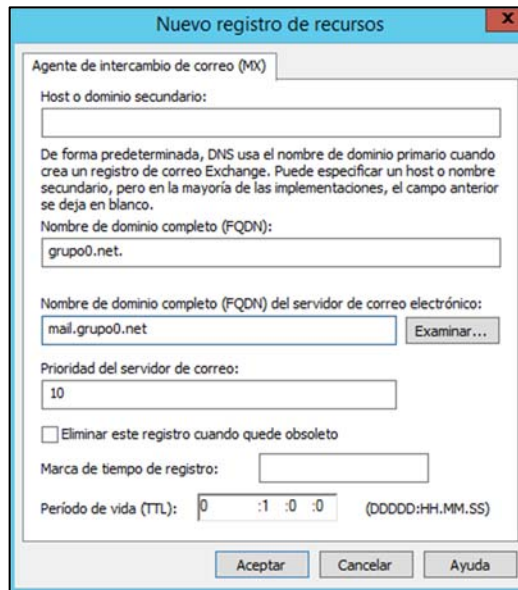
A continuación creamos dos registros del tipo CNAME, que permiten crear alias para un nombre de la forma siguiente:



Seleccionamos la opción “Alias nuevo (CNAME)...”. Hemos de crear dos registros con alias *pop* y *smtp*, que apuntan hacia mail.grupoXX.net.

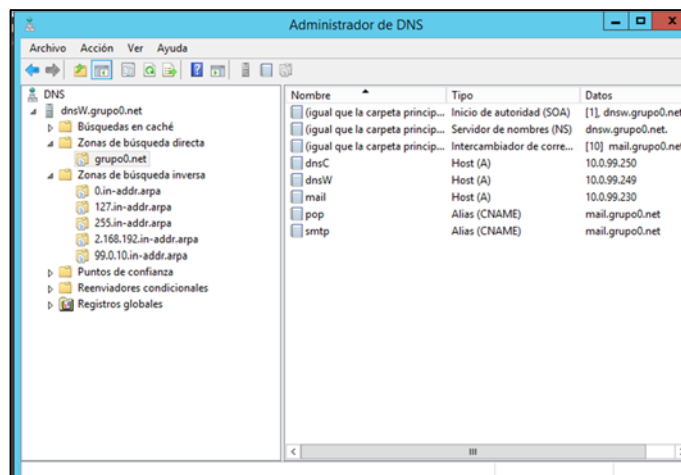



A continuación creamos un registro del tipo MX que permite indicar el servidor de correo para el dominio. Este registro es consultado por el servidor de correo electrónico para hacer entrega de correo a los destinatarios. Para ello, hemos de clicar con el botón derecho del ratón, sobre grupoXX.net. Seleccionaremos la opción “Nuevo intercambio de correo (MX)”:



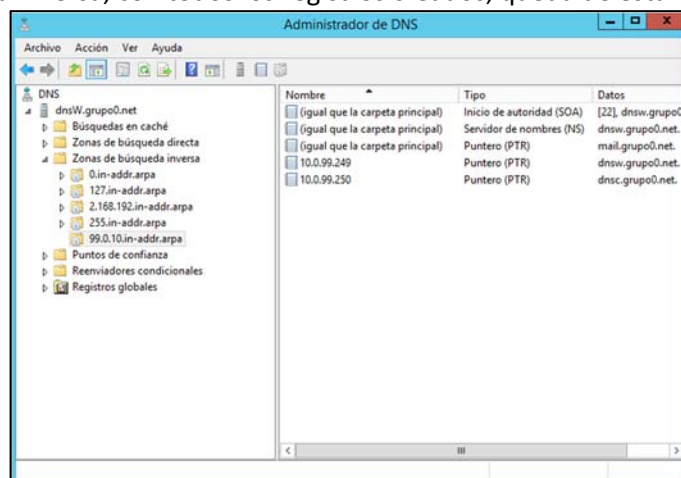
Rellenamos el formulario indicando que el servidor es el *mail.grupoXX.net*

En la figura siguiente podemos ver cómo nos queda la zona de búsqueda directa con todos los registros creados:



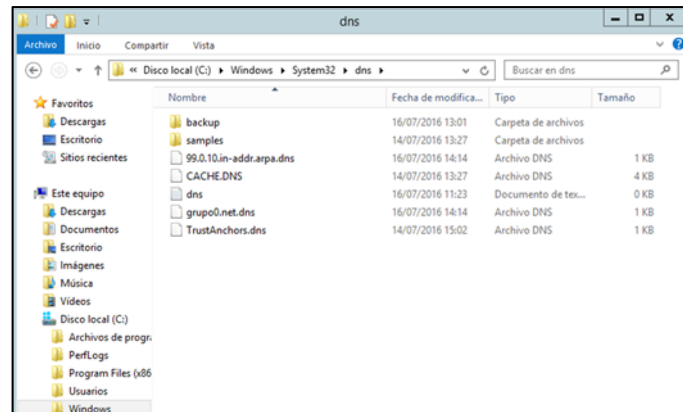
Nombre	Tipo	Datos
(igual que la carpeta princip...	Inicio de autoridad (SOA)	[1] dnsW.grupo0.net.
(igual que la carpeta princip...	Servidor de nombres (NS)	dnsW.grupo0.net.
(igual que la carpeta princip...	Intercambiador de corre...	[10] mail.grupo0.net
dnsC	Host (A)	10.0.99.250
dnsW	Host (A)	10.0.99.249
mail	Host (A)	10.0.99.230
pop	Alias (CNAME)	mail.grupo0.net
smtp	Alias (CNAME)	mail.grupo0.net

La zona de búsqueda inversa, con todos los registros creados, queda de esta manera:



Nombre	Tipo	Datos
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[22] dnsW.grupo0.
(igual que la carpeta principal)	Servidor de nombres (NS)	dnsW.grupo0.net.
(igual que la carpeta principal)	Puntero (PTR)	mail.grupo0.net.
10.0.99.249	Puntero (PTR)	dnsW.grupo0.net.
10.0.99.250	Puntero (PTR)	dnsC.grupo0.net.

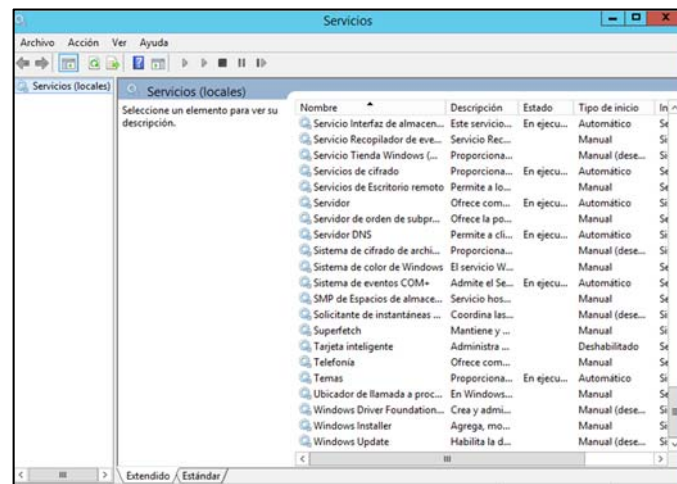
Accediendo al Explorador de Windows, clic Inicio→Este equipo→Disco Local (C:)→Windows→System32→dns:



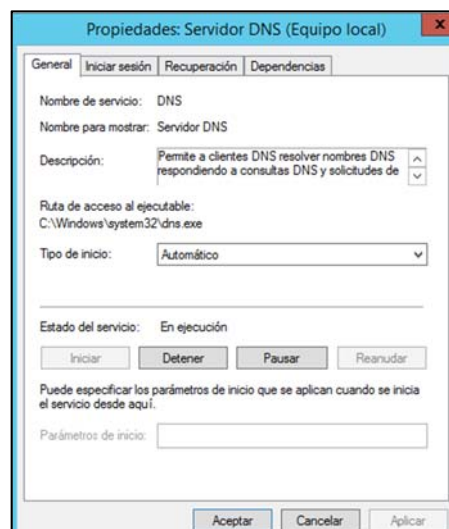
Encontramos una serie de registros que son actualizados periódicamente por el servidor. En caso que, no estén actualizados podemos forzar esta actualización reiniciando el servicio.

Dos formas de reiniciar el servicio:

Inicio→Herramientas Administrativas→Servicios→Servidor DNS



Al hacer clic en Servidor DNS, se abre una ventana, daremos a Detener y posteriormente a Iniciar.



O bien desde la ventana de comandos. Introducimos el comando net start. Con ello tendremos todos los servicios activos.

```
PS C:\Users\Administrador> net start
Se han iniciado estos servicios de Windows:
Administración de aplicaciones
Administración remota de Windows (WS-Management)
Administrador de conexiones de Windows
Administrador de cuentas de seguridad
Administrador de sesión local
Agente de eventos del sistema
Aplicación auxiliar de NetBIOS sobre TCP/IP
Aplicación auxiliar IP
Asignador de extremos de RPC
Cliente de directiva de grupo
Cliente de seguimiento de vínculos distribuidos
Cliente DHCP
Cola de impresión
Conexiones de red
Coordinador de transacciones distribuidas
Detección de hardware shell
Energía
Estación de trabajo
Firewall de Windows
Hora de Windows
Iniciador de procesos de servidor DCOM
Instrumental de administración de Windows
Llamada a procedimiento remoto (RPC)
Motor de filtrado de base
Plug and Play
Programador de tareas
Protección de software
Reconec. ubicación de red
Registro de eventos de Windows
Servicio de caché de fuentes de Windows
Servicio de directivas de diagnóstico
Servicio de infraestructura de tareas en segundo plano
Servicio de lista de redes
Servicio de notificación de eventos de sistema
Servicio de perfil de usuario
Servicio de registro de acceso de usuarios
Servicio Interfaz de almacenamiento en red
Servicios de cifrado
Servidor
Servidor DNS
Sistema de eventos COM+
Temas
Se ha completado el comando correctamente.
PS C:\Users\Administrador>
```

Vemos que tenemos “Servidor DNS”, Ejecutamos net stop “Servidor DNS” y posteriormente net start “Servidor DNS”.

```
PS C:\Users\Administrador> net stop "Servidor DNS"
El servicio de Servidor DNS está deteniéndose.
El servicio de Servidor DNS se detuvo correctamente.

PS C:\Users\Administrador> net start "Servidor DNS"
El servicio de Servidor DNS está iniciándose.
El servicio de Servidor DNS se ha iniciado correctamente.

PS C:\Users\Administrador> _
```

Ya actualizado, en su caso, observamos en la carpeta dns, el fichero grupo0.net.dns donde se encuentra la configuración de la zona directa:

```
grupo0.net.dns: Bloc de notas
Archivo Edición Formato Ver Ayuda
;
; Database file grupo0.net.dns for Default zone scope in zone grupo0.net.
; Zone version: 21
;
;
@           IN      SOA     dnsw.grupo0.net. hostmaster.grupo0.net. (
                                21           ; serial number
                                900          ; refresh
                                600         ; retry
                                86400       ; expire
                                3600        ) ; default TTL
;
; Zone NS records
;
@           IN      NS      dnsw.grupo0.net.
;
; Zone records
;
@           IN      MX      10      mail.grupo0.net.
dnsC        IN      A       10.0.99.250
dnsw        IN      A       10.0.99.249
mail        IN      A       10.0.99.230
pop         IN      CNAME   mail.grupo0.net.
smtp        IN      CNAME   mail.grupo0.net.
```

Y por otro lado se encuentra el fichero 99.0.10.in-addr.arpa donde aparece toda la configuración de la zona inversa.

```
99.0.10.in-addr.arpa: Bloc de notas
Archivo Edición Formato Ver Ayuda
;
; Database file 99.0.10.in-addr.arpa.dns for Default zone scope in zone 99.0.10.in-addr.arpa.
; Zone version: 22
;
@           IN      SOA  dnsw.grupo0.net. hostmaster.grupo0.net. (
                22      ; serial number
                900     ; refresh
                600     ; retry
                86400   ; expire
                3600    ) ; default TTL
;
; Zone NS records
;
@           IN      NS   dnsw.grupo0.net.
;
; Zone records
;
230        PTR    mail.grupo0.net.
249        PTR    dnsw.grupo0.net.
250        PTR    dnsC.grupo0.net.
```

A continuación se comprueba el funcionamiento con un cliente. Para ello abrimos el cliente SO Windows 8.1 usado en la práctica DHCP. Recuerde configurar la IP estática y desde él abra la ventana de Shell. Botón derecho Inicio → Símbolo del Sistema.

```
Símbolo del sistema - nslookup
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.
C:\Users\Pablo Bernabeu>nslookup
Servidor predeterminado: dnsw.grupo0.net
Address: 10.0.99.249
> dnsW.grupo0.net
Servidor: dnsw.grupo0.net
Address: 10.0.99.249
Nombre: dnsW.grupo0.net
Address: 10.0.99.249
> dnsC.grupo0.net
Servidor: dnsw.grupo0.net
Address: 10.0.99.249
Nombre: dnsC.grupo0.net
Address: 10.0.99.250
>
```

```
Símbolo del sistema - nslookup
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.
C:\Users\Pablo Bernabeu>nslookup
Servidor predeterminado: dnsw.grupo0.net
Address: 10.0.99.249
> www.google.es
Servidor: dnsw.grupo0.net
Address: 10.0.99.249
Nombre: www.google.es
Addresses: 2a00:1450:400c:c04::5e
          74.125.206.94
> www.upv.es
Servidor: dnsw.grupo0.net
Address: 10.0.99.249
Respuesta no autoritativa:
Nombre: ias.cc.upv.es
Address: 158.42.4.23
Alias: www.upv.es
>
```

Introduciendo el comando *nslookup* se pueden consultar los registros del servicio DNS, tal como se puede ver en las pantallas anteriores, se pueden consultar los registros de la zona de resolución inversa o directa.

Es importante destacar que, cuando se hace una consulta de una dirección de fuera del dominio que controla el servidor DNS, este indica que la respuesta es *Non Authoritative*, esto nos indica que la ha obtenido mediante una consulta a otro servidor.

Para consultar los registros NS del dominio, se indica el tipo de consulta y el dominio. Para los registros MX del dominio, también se indica el tipo de consulta y el dominio. Tal como podemos observar en la siguiente imagen.


```
Símbolo del sistema - nslookup
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.
C:\Users\Pablo Bernabeu>nslookup
Servidor predeterminado: dns.w.grupo0.net
Address: 10.0.99.249

> set querytype=NS
> grupo0.net
Servidor: dns.w.grupo0.net
Address: 10.0.99.249

grupo0.net      nameserver = dns.w.grupo0.net
dns.w.grupo0.net internet address = 10.0.99.249
> set querytype=MX
> grupo0.net
Servidor: dns.w.grupo0.net
Address: 10.0.99.249

grupo0.net      MX preference = 10, mail exchanger = mail.grupo0.net
mail.grupo0.net internet address = 10.0.99.230
>
```

5. Configuración del Servidor Secundario en Centos 7

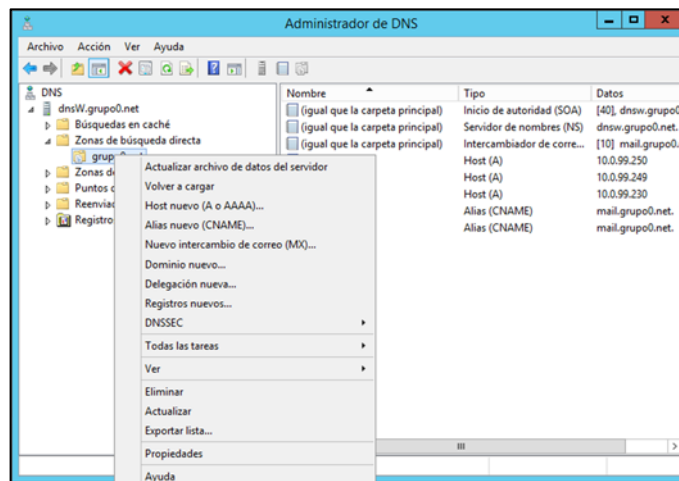
Configure el servidor DNS en Centos Red Had7 tal como se indica en la práctica de configuración del Servidor Centros DNS en Centos.

Una vez realizada la misma continúe en el punto 8 de la presente práctica.

6. Configuración para el funcionamiento con dos servidores DNS: principal (Windows 2012 server) y secundario (Centos 7)

El primer paso es indicar al servidor principal DNSW que hay un servidor secundario, para darle permiso de compartición de la base de datos. Por lo tanto, primero se ha de preparar el servidor principal.

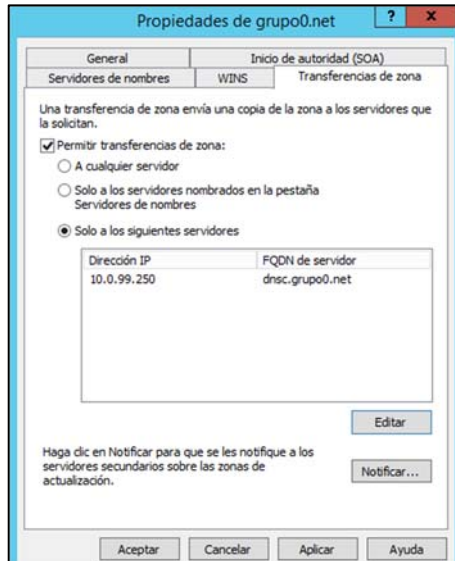
En el Panel de Administrador del Servidor → DNS → Zonas de búsqueda directa → grupoXX.net, y a continuación clic en el botón derecho del ratón:



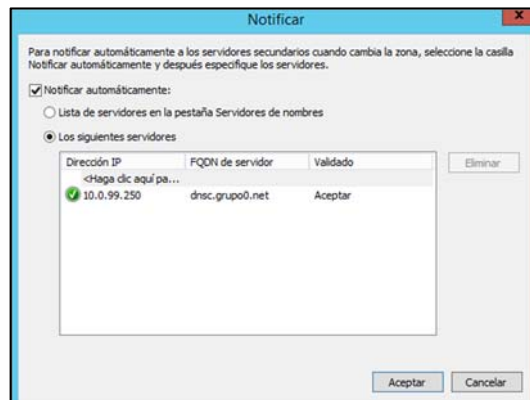
Seleccionamos la opción Propiedades:

Nos aparece una ventana donde encontramos las propiedades de la zona directa grupo0.net, con diferentes pestañas, seleccionamos la pestaña Transferencias de Zona.

En este pestaña indicamos las opciones Permitir transferencias de zona y solo a los siguientes servidores. A continuación clic en editar e introducimos la dirección IP de nuestro servidor DNSC, 10.XX.99.250.

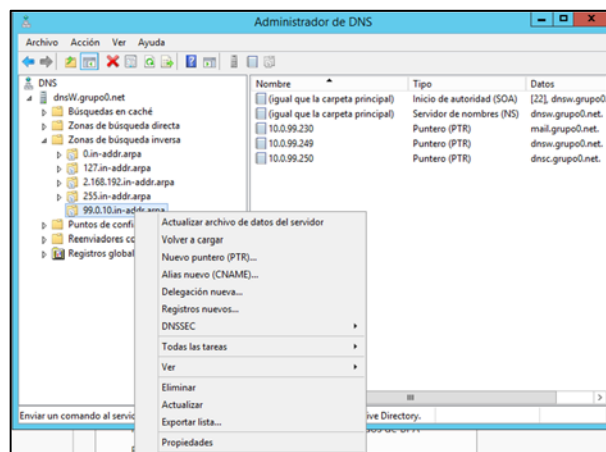


Una vez editado, clic en Notificar, y le indicamos notifique a nuestro servidor secundario.

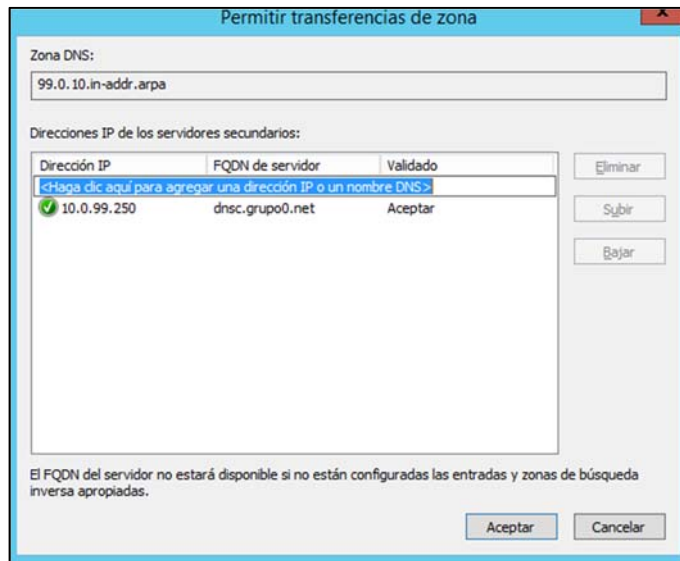


El paso siguiente, antes de configurar el servidor secundario, es realizar los mismos pasos, pero para la zona de búsqueda inversa.

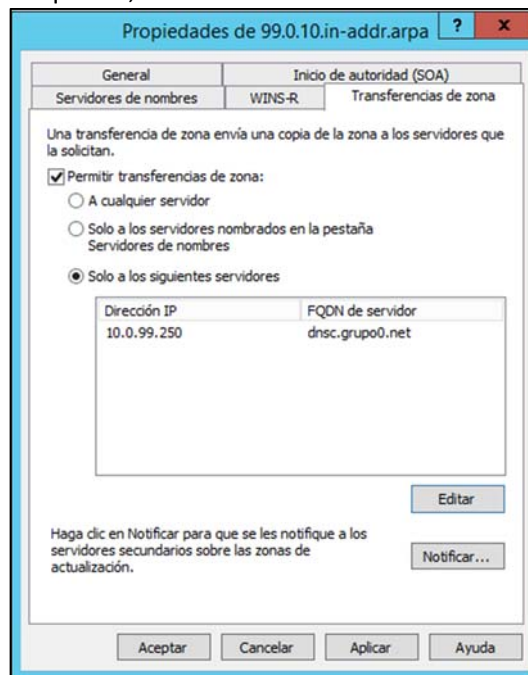
Zona de búsqueda inversa → 99.0.10.in-addr.arpa (clic botón derecho del ratón y seleccionamos propiedades).



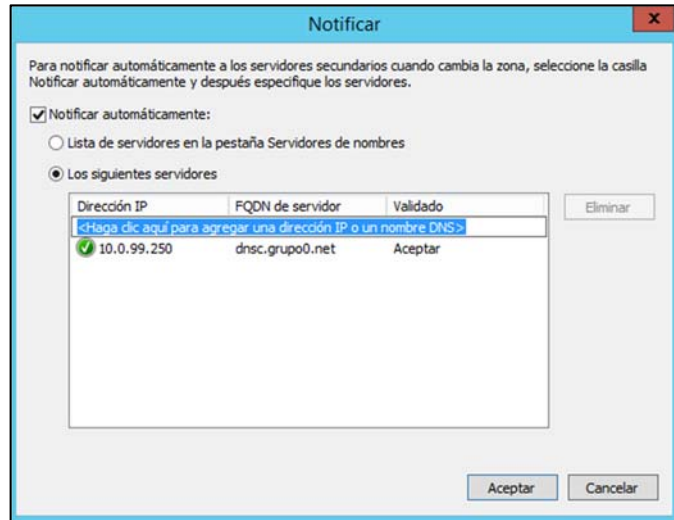
Aparece las propiedades de la zona inversa nombrada 99.0.in-addr.arpa. Seleccionamos la pestaña “Transferencia de Zona”, marcamos la opción “Sólo a los siguientes servidores” y clicamos en Editar:



Damos en aceptar y nos deberá quedar,



Clicaremos en Notificar. El motivo, hemos de indicarle al servidor secundario que en cada ocasión que haya algún cambio, debe indicarlo.



Damos dos veces a aceptar y daremos por concluida la configuración del servidor principal en Windows.

En el servidor secundario se ha de indicar quien es el servidor principal del dominio. Vayamos al punto 6 de la Práctica: Configuración Servidor DNS en Centos 7.

7. Configurar un servidor Windows 2012 r2 como secundario, siendo servidor Centos Principal

Antes de realizar este punto debéis hacer el punto 7 de la Práctica: “Configuración Servidor DNS en Centos 7”.

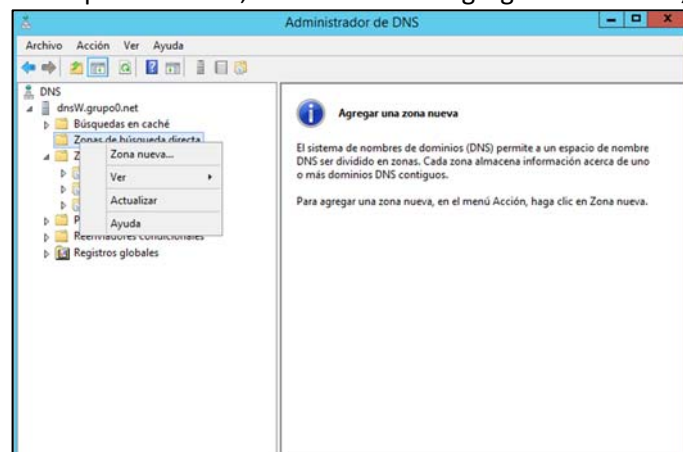
Llegado a este punto ya tenemos configurado el servidor Centos como principal. Queda pues configurar éste como secundario.

Administrador DNS→Zona de búsqueda directa, clic, botón derecho→Eliminamos la zona tenemos grupo0.net (estaba creada como principal y debemos quitarla).

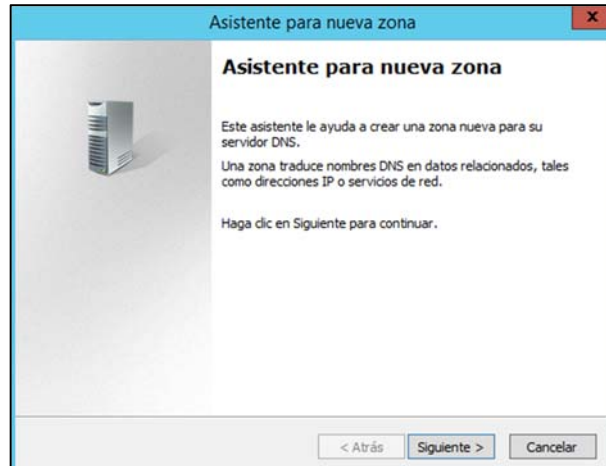
Hacemos lo mismo para la zona inversa. Eliminamos 99.0.10.in-addr.arpa

De esta forma lo dejamos cómo si lo estuviésemos configurando por primera vez.

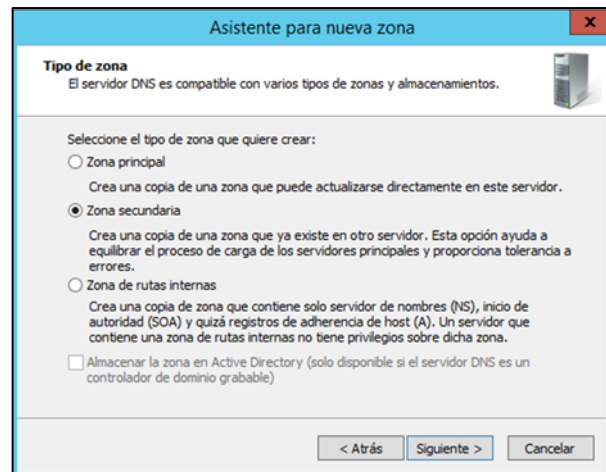
Volvemos a Zona de búsqueda directa, botón derecho. Agregar zona nueva,



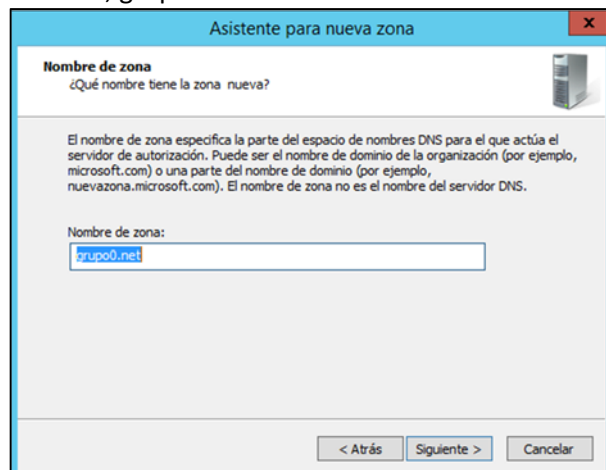
Y nos aparecerá el asistente para Zona Nueva:



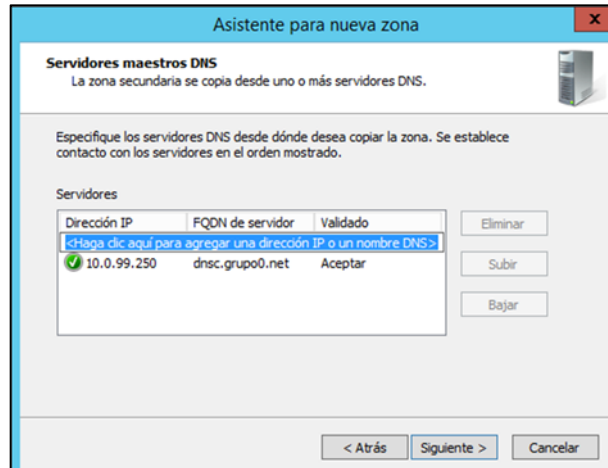
Clicamos en siguiente y le indicamos que la zona que se quiere crear es Zona Secundaria. Hacemos clic en siguiente.



Le ponemos de nombre de zona, grupoXX.net:

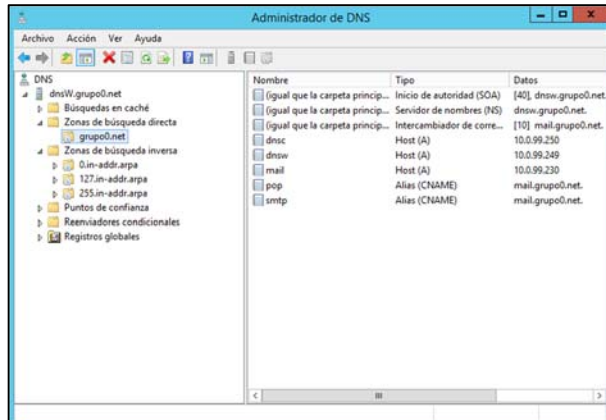


Clic en siguiente e indicamos la IP del Servidor principal 10.XX.99.250.



Damos a siguiente y a Finalizar.

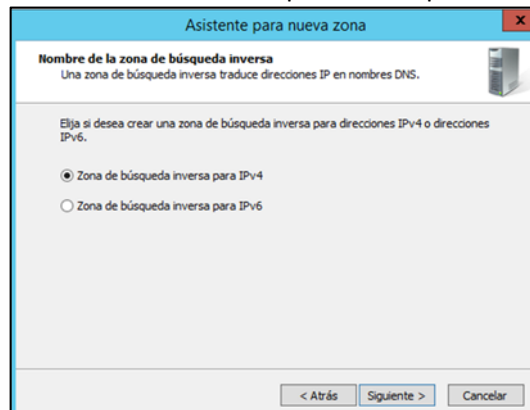
Si hacemos clic en grupo0.net, vemos que ya ha recibido la BBDD:



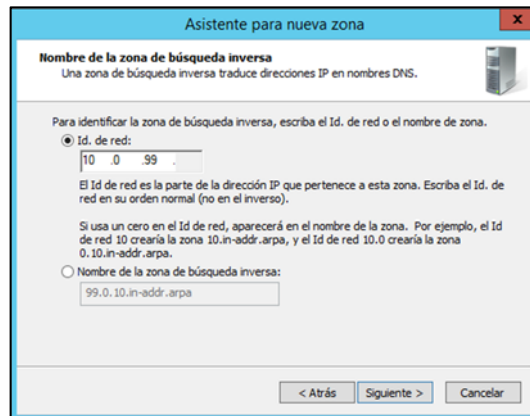
Ahora hemos de proceder de la misma forma para la zona inversa.

Zona de búsqueda inversa → Botón derecho → Zona Nueva,

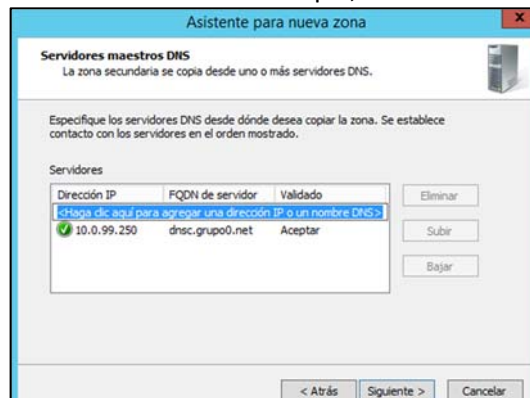
Se nos abre el asistente damos a siguiente y seleccionamos Zona Secundaria, damos a siguiente, en esta pantalla se nos pide si la zona inversa es para IPv4 o para IPv6.



Seleccionamos IPv4 y damos a siguiente. Identificamos a la red 10.XX.99:

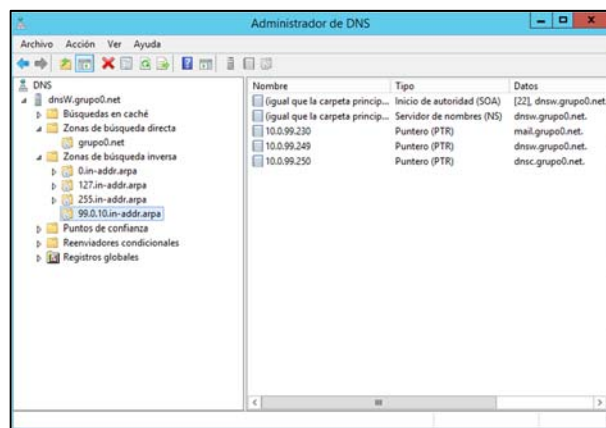


Clic en siguiente y le damos la IP del servidor Principal, 10.XX.99.250



Clic en siguiente y finalizar.

Si ahora hacemos clic en 99.0.10.in-addr.arpa vemos que ya ha recibido la BBDD del servidor Principal



Verificad el correcto funcionamiento.