

Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR

Requisitos previos: Tener instalado un sistema de virtualización en este caso VirtualBox y tener a disposición los siguientes sistemas Windows 7 y Server 2008R2, pfSense y Debian.

Descripción de la práctica: Instalar el rol de servicio DNS en W2008R2, configurar el reenvío de resolución DNS y la resolución directa.

Descripción de Hardware: Equipo real, Intel Core i7 con 16GB de RAM y 199GB de disco duro

Esquema de la Red

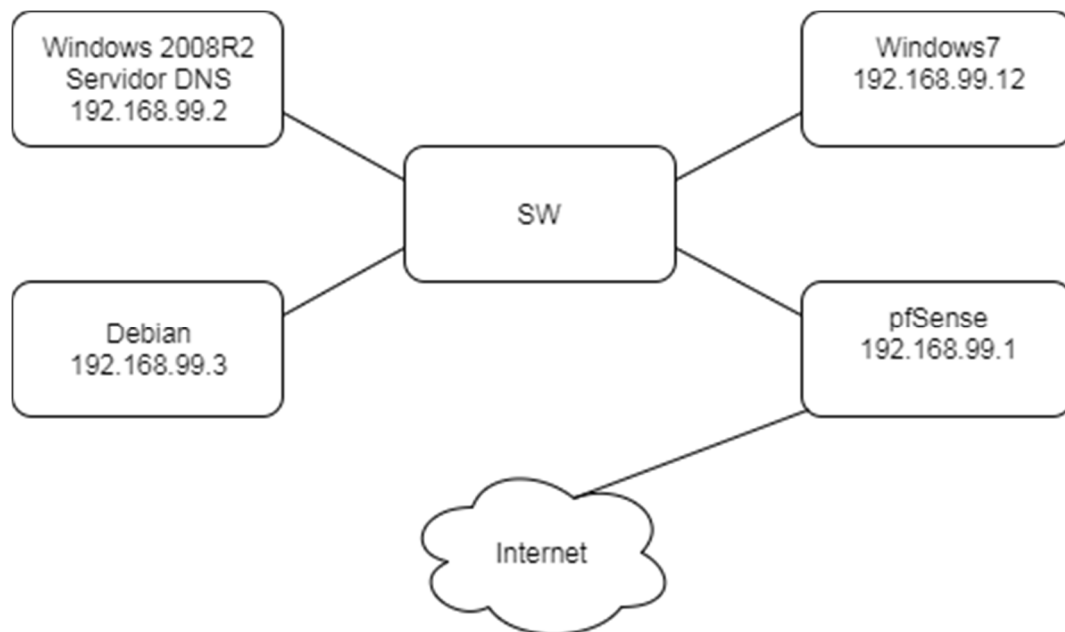
Rangos de direcciones:

192.168.99.2 – Windows 2008R2 (Servidor DNS)

192.168.99.1 – pfSense

192.168.99.12 – Windows 7

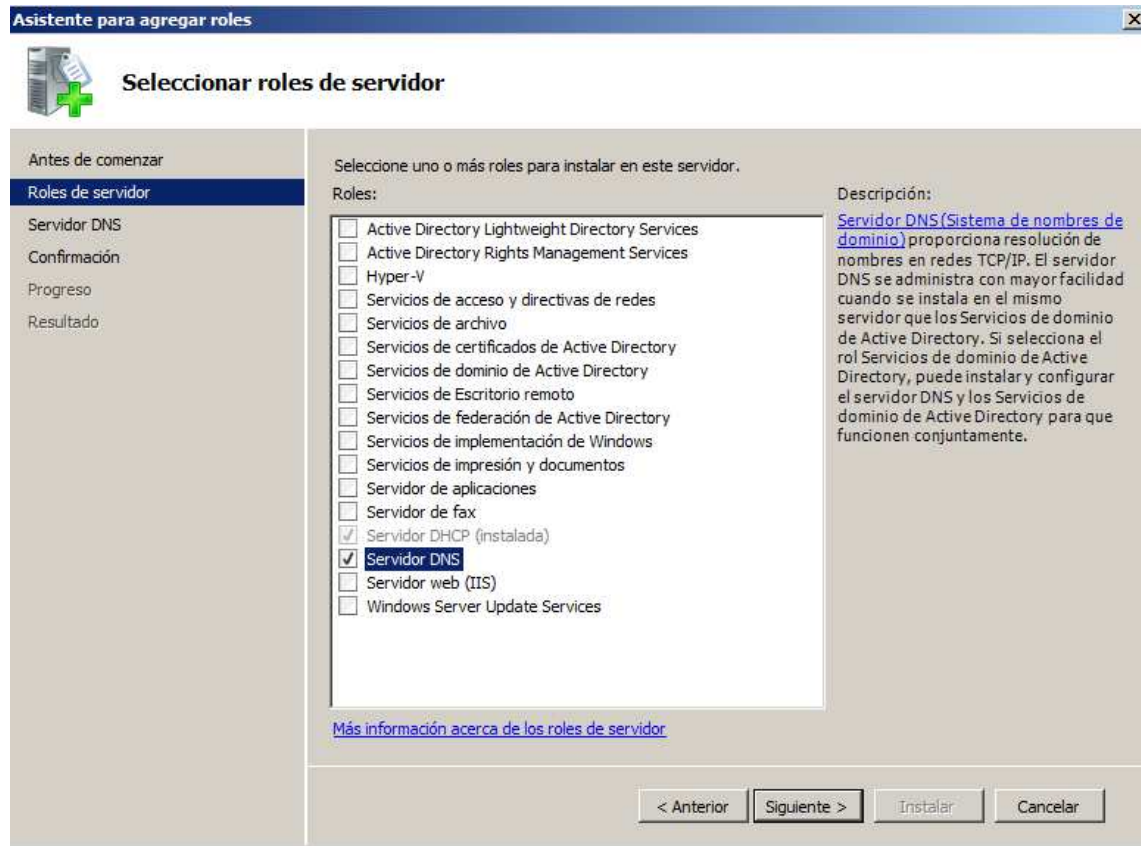
192.168.99.3 – Debian



Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR

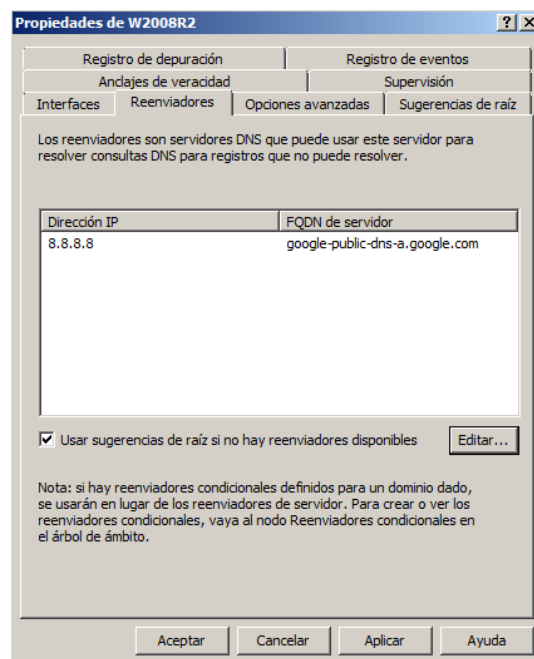
Comenzamos instalando el rol de servidor DNS en W2008R2 (clicar en siguiente en todas las pestañas)



Con el servidor sin configurar, vamos a activar el reenvío para que las peticiones que 2008R2 no pueda resolver las resuelva en 8.8.8.8.

Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR



Observamos la diferencia de configurar el reenvío con nslookup en Windows 7. (previamente cambiamos el servidor DNS a 192.168.99.2 que es la IP de W2008R2)

```
C:\Windows\system32\cmd.exe
C:\Users\seg>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\Users\seg>nslookup www.marca.com
Servidor: UnKnown
Address: 192.168.99.2

Respuesta no autoritativa:
Nombre: www.marca.com
Addresses: 2001:67c:2294:1000::f109
193.110.128.109

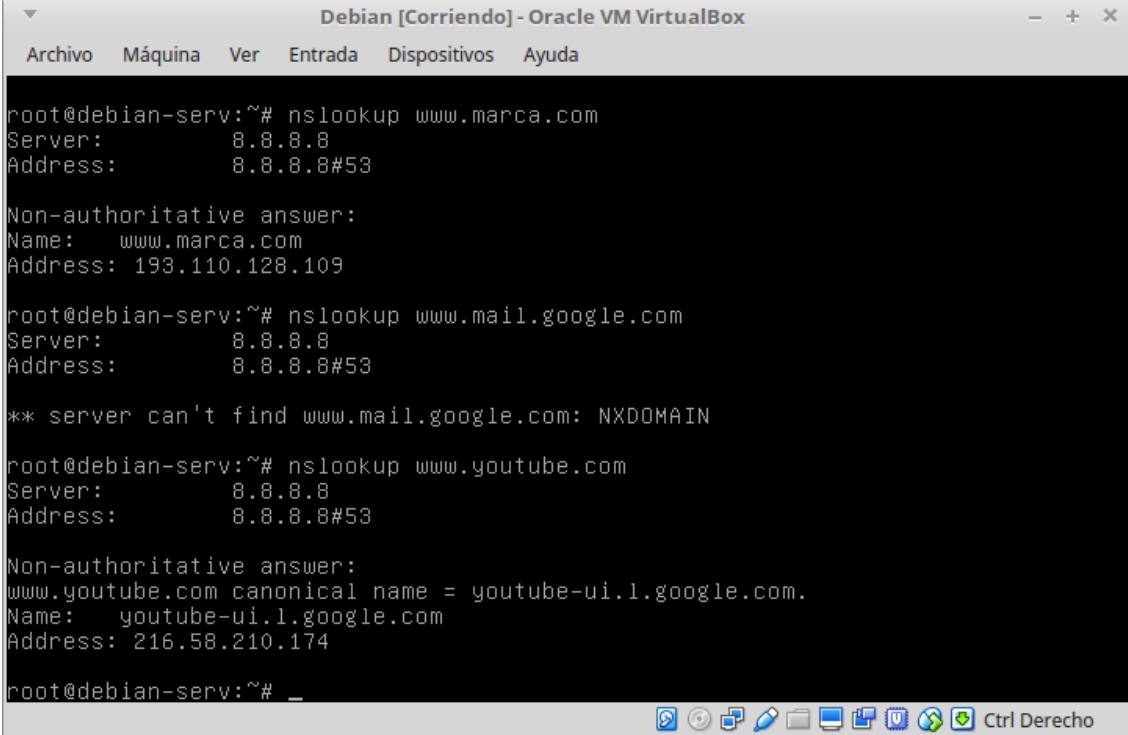
C:\Users\seg>nslookup www.youtube.com
Servidor: UnKnown
Address: 192.168.99.2

Respuesta no autoritativa:
Nombre: youtube-ui.l.google.com
Addresses: 2a00:1450:4003:807::200e
216.58.210.174
Aliases: www.youtube.com
```

Antes de hacer la prueba en Debian, cambiamos el archivo /etc/resolv.conf y le damos como servidor DNS la IP de W2008R2

Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR



```
Debian [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

root@debian-serv:~# nslookup www.marca.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   www.marca.com
Address: 193.110.128.109

root@debian-serv:~# nslookup www.mail.google.com
Server:      8.8.8.8
Address:     8.8.8.8#53

** server can't find www.mail.google.com: NXDOMAIN

root@debian-serv:~# nslookup www.youtube.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.youtube.com canonical name = youtube-ui.l.google.com.
Name:   youtube-ui.l.google.com
Address: 216.58.210.174

root@debian-serv:~# _
```

Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR

Realizamos un nslookup a debian.asir.x , es decir queremos saber cuál es la IP de debian.asir.x

```
Respuesta no autoritativa:
Nombre: www.marca.com
Addresses: 2001:67c:2294:1000::f109
          193.110.128.109

C:\Users\seg>nslookup debian.asir.net
Servidor: UnKnown
Address: 192.168.99.2

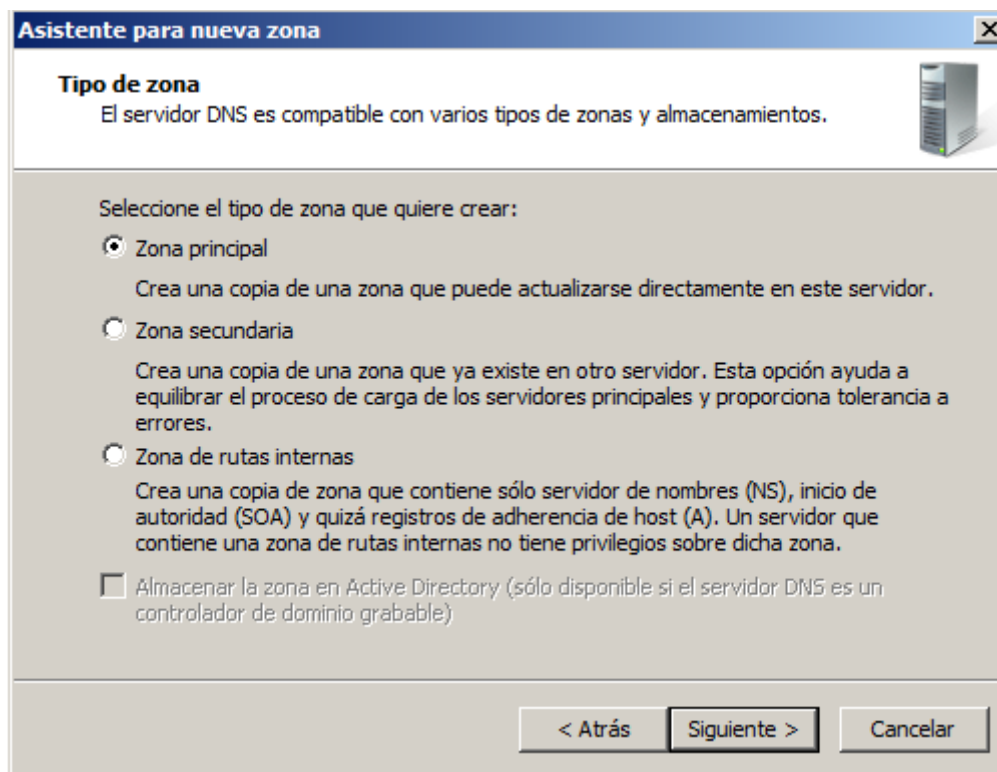
Respuesta no autoritativa:
Nombre: debian.asir.net
Address: 207.148.248.143

C:\Users\seg>nslookup debian.asir.x
Servidor: UnKnown
Address: 192.168.99.2

*** UnKnown no encuentra debian.asir.x: Non-existent domain
C:\Users\seg>
```

En la respuesta vemos que el servidor DNS no resuelve la petición, por lo tanto vamos a crear una Zona de resolución directa.

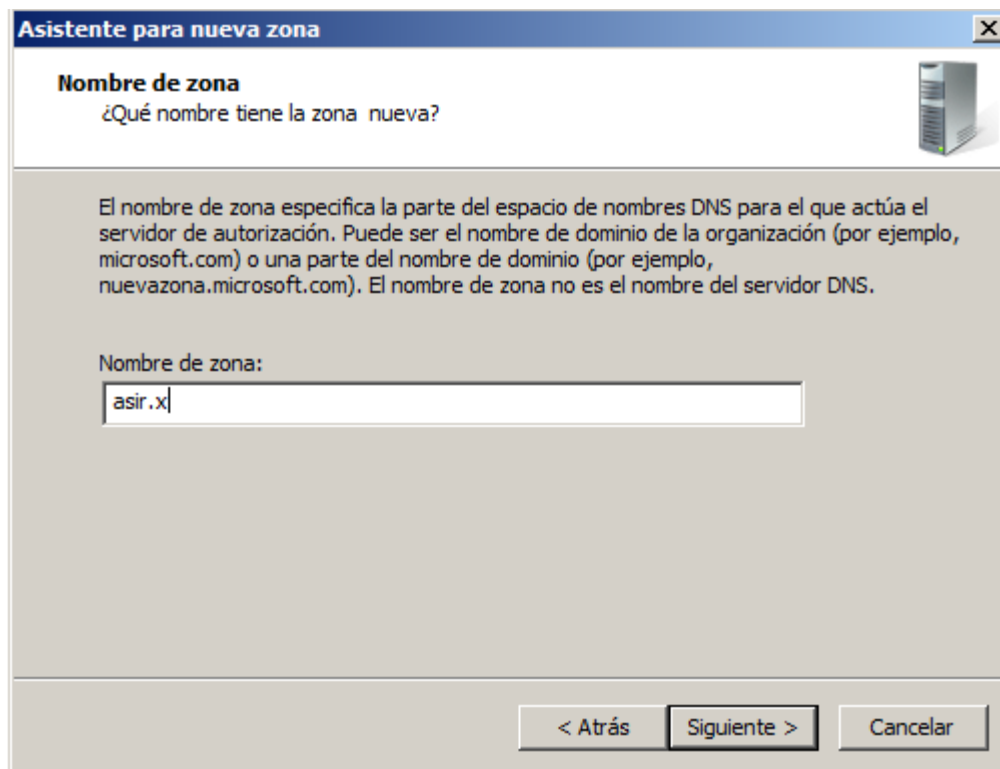
Lo crearemos como Zona principal.



Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR

Escogemos el nombre de la zona: asir.x



Asistente para nueva zona

Nombre de zona
¿Qué nombre tiene la zona nueva?

El nombre de zona especifica la parte del espacio de nombres DNS para el que actúa el servidor de autorización. Puede ser el nombre de dominio de la organización (por ejemplo, microsoft.com) o una parte del nombre de dominio (por ejemplo, nuevazona.microsoft.com). El nombre de zona no es el nombre del servidor DNS.

Nombre de zona:

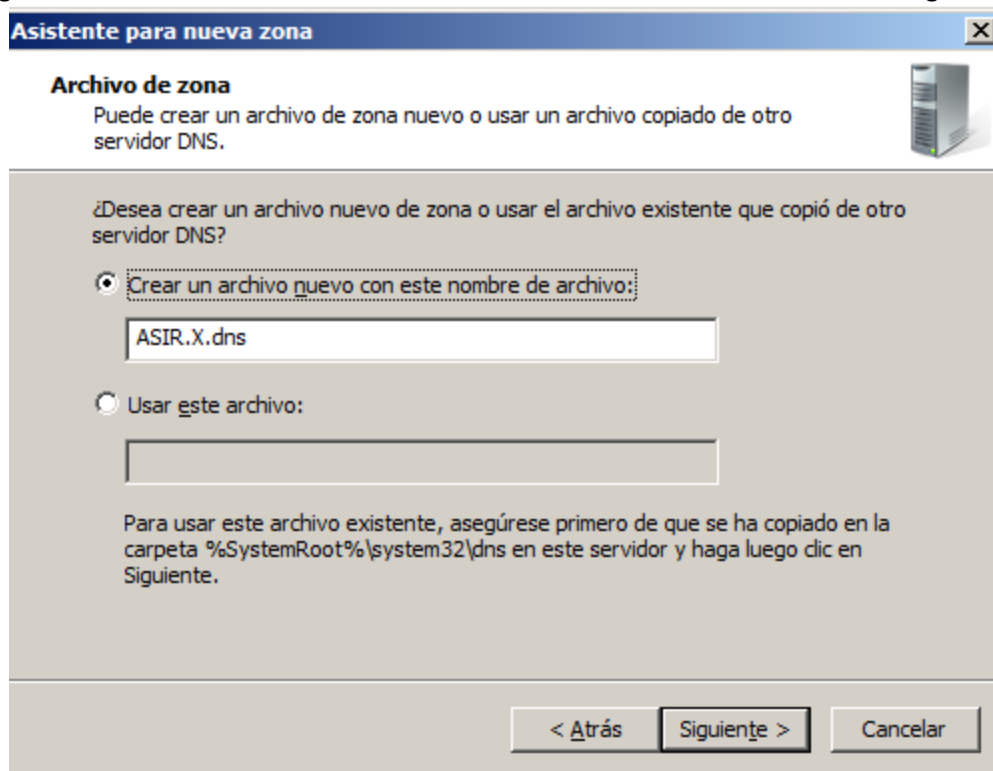
asir.x

< Atrás Siguiendo > Cancelar

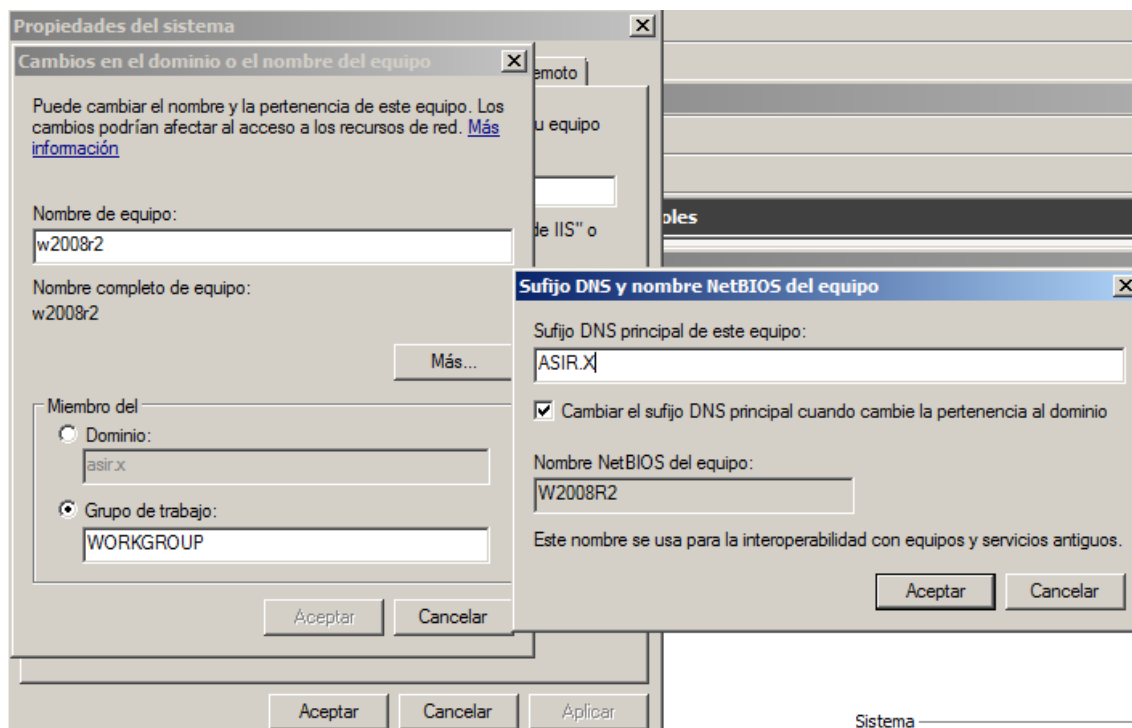
Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR

Escogemos el nombre del archivo donde se va a almacenar la información de configuración.



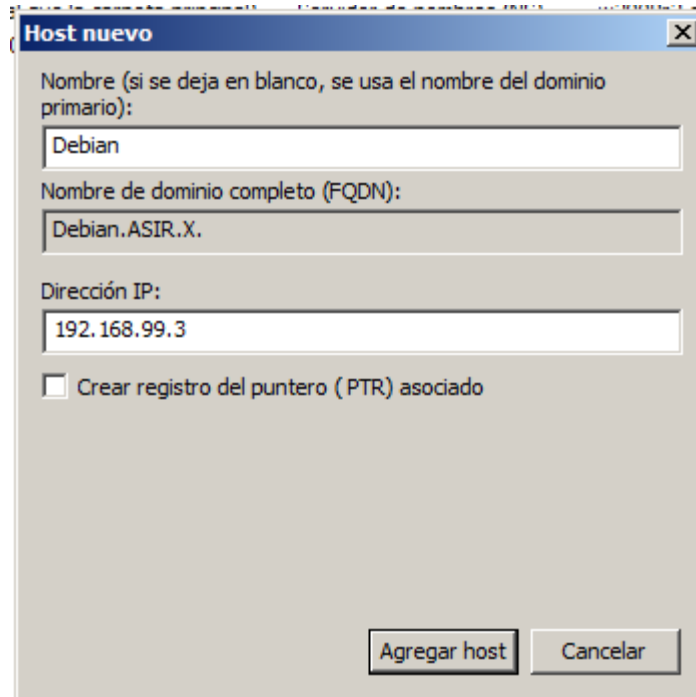
Cambiamos el sufijo DNS de Windows 2008R2, quedaría algo así. W2008R2.ASIR.X



Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR

Agregamos los punteros A (hosts) para que DNS resuelva el nombre debian.asir.x , también añadiremos los demás equipos de la red.



Ahora vemos como la petición nslookup debian.asir.x desde Windows 7 es resuelta por el

```
C:\Windows\system32\cmd.exe

C:\Users\seg>nslookup debian.asir.net
Servidor: Unknown
Address: 192.168.99.2

Respuesta no autoritativa:
Nombre: debian.asir.net
Address: 207.148.248.143

C:\Users\seg>nslookup debian.asir.x
Servidor: Unknown
Address: 192.168.99.2

*** Unknown no encuentra debian.asir.x: Non-existent domain

C:\Users\seg>nslookup debian.asir.x
Servidor: Unknown
Address: 192.168.99.2

Nombre: debian.asir.x
Address: 192.168.99.3

C:\Users\seg>
```

servidor.

Lo mismo ocurre con windows7.asir.x desde Debian

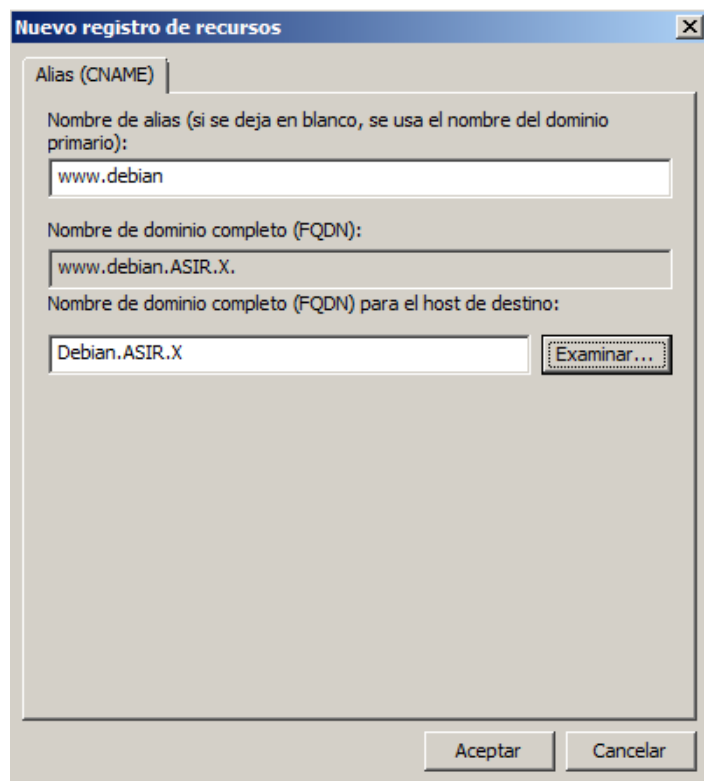
Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR

```
root@debian-serv:~# nslookup windows7.asir.x
Server:      192.168.99.2
Address:     192.168.99.2#53

Name:   windows7.asir.x
Address: 192.168.99.12
root@debian-serv:~# _
```

Ahora vamos a añadir una entrada CNAME (alias) para Debian, con esta entrada el servidor responderá a las peticiones nslookup www.debian.asir.x



Hacemos la comprobación desde Windows 7.

```
C:\Windows\system32\cmd.exe
programa o archivo por lotes ejecutable.

C:\Users\seg>ping www.debian.asir.x

Haciendo ping a debian.asir.x [192.168.99.3] con 32 bytes de datos:
Respuesta desde 192.168.99.3: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.99.3: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.99.3:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    <0% perdidos>,
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\seg>nslookup www.debian.asir.x
Servidor:  UnKnown
Address:   192.168.99.2

Nombre:   debian.asir.x
Address:  192.168.99.3
Alias(es): www.debian.asir.x

C:\Users\seg>
```

Windows 2008R2 Configurar reenvío y resolución directa DNS

David Sora – 2ASIR

Vemos en profundidad la respuesta del servidor desde Debian con el comando dig

```
root@debian-serv:~# dig www.asir.x

; <<>> DiG 9.9.5-9+deb8u13-Debian <<>> www.asir.x
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 32200
; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; QUESTION SECTION:
;www.asir.x.                IN      A

; AUTHORITY SECTION:
asir.x. 3600      IN      SOA      w2008r2.asir.x. hostmaster.asir.
x. 4 900 600 86400 3600

; Query time: 7 msec
; SERVER: 192.168.99.2#53(192.168.99.2)
; WHEN: Fri Oct 20 11:09:11 CEST 2017
; MSG SIZE rcvd: 100

root@debian-serv:~#
```