CENTRE ESPECÍFIC
D´EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

# UNIT 2.
# TO KNOW MORE ACTIVITY

**Web Applications Deployment**
**CFGS DAW**

## Important: the content of this activity is not for exam

Carlos Cacho López
carlos.cacho@ceedcv.es
2018/2019

## License



## Nomenclature

During this unit we are going to use special symbols to distinct some important elements.

This symbols are:

 Important

 Attention

 Interesting

# INDEX

# UT02. SERVICES INVOLVED IN WEB DEPLOYMENT
# TO KNOW MORE ACTIVITY

## 1. INTRODUCTION

This is an extra activity just to know more about DNS, FTP and SSH. We are going to install and configure two DNS servers (one in windows and the other in Linux). Then we are going to install and configure a FTP and SSH server in Linux.

## 2. DNS

### 2.1 Installing and configuring cache-only DNS server in WS2016

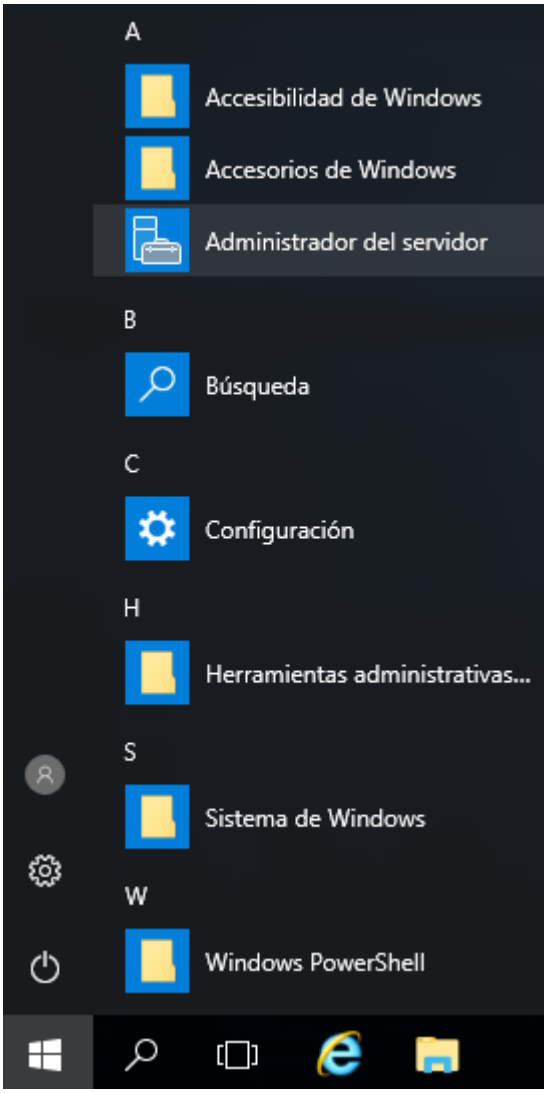
We are going to install and configure a DNS server in our *windowsServer* to use it as an **only-cache** DNS which answers recursive queries.

#### 2.1.1 Installing the DNS server

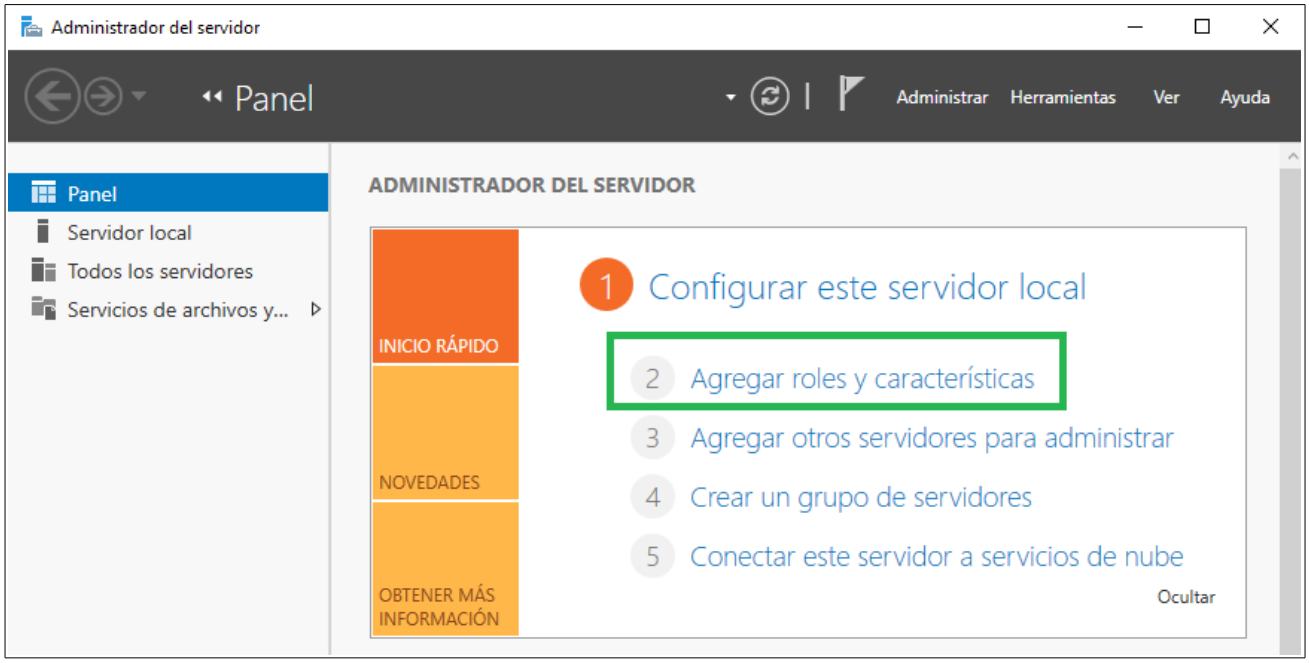
To install a DNS server in Windows Server 2016 you have to follow these steps:

1. Start session at *windowsServer* virtual machine with the administrator user.

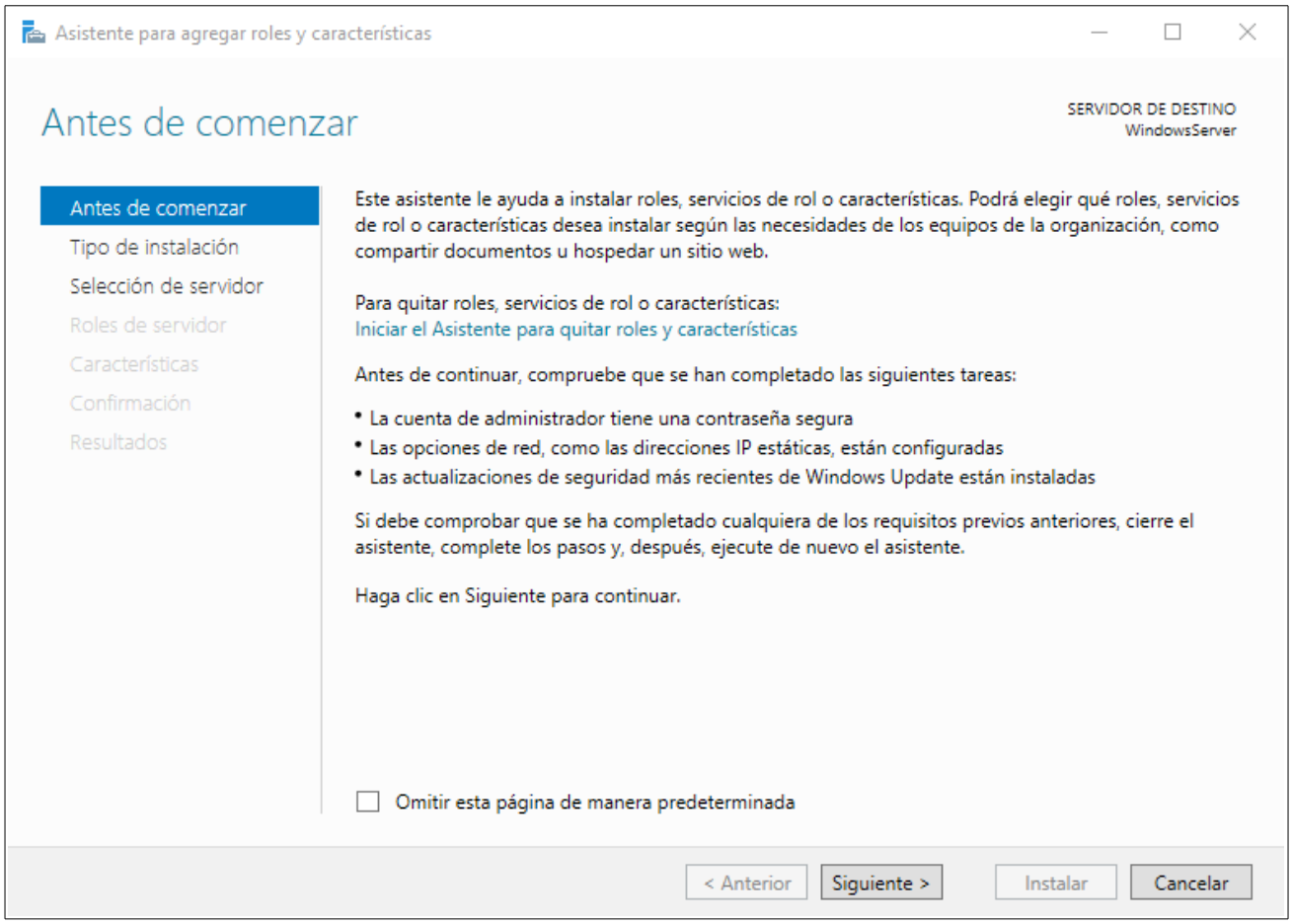
2. Click on ***START MENU > SERVER MANAGER***



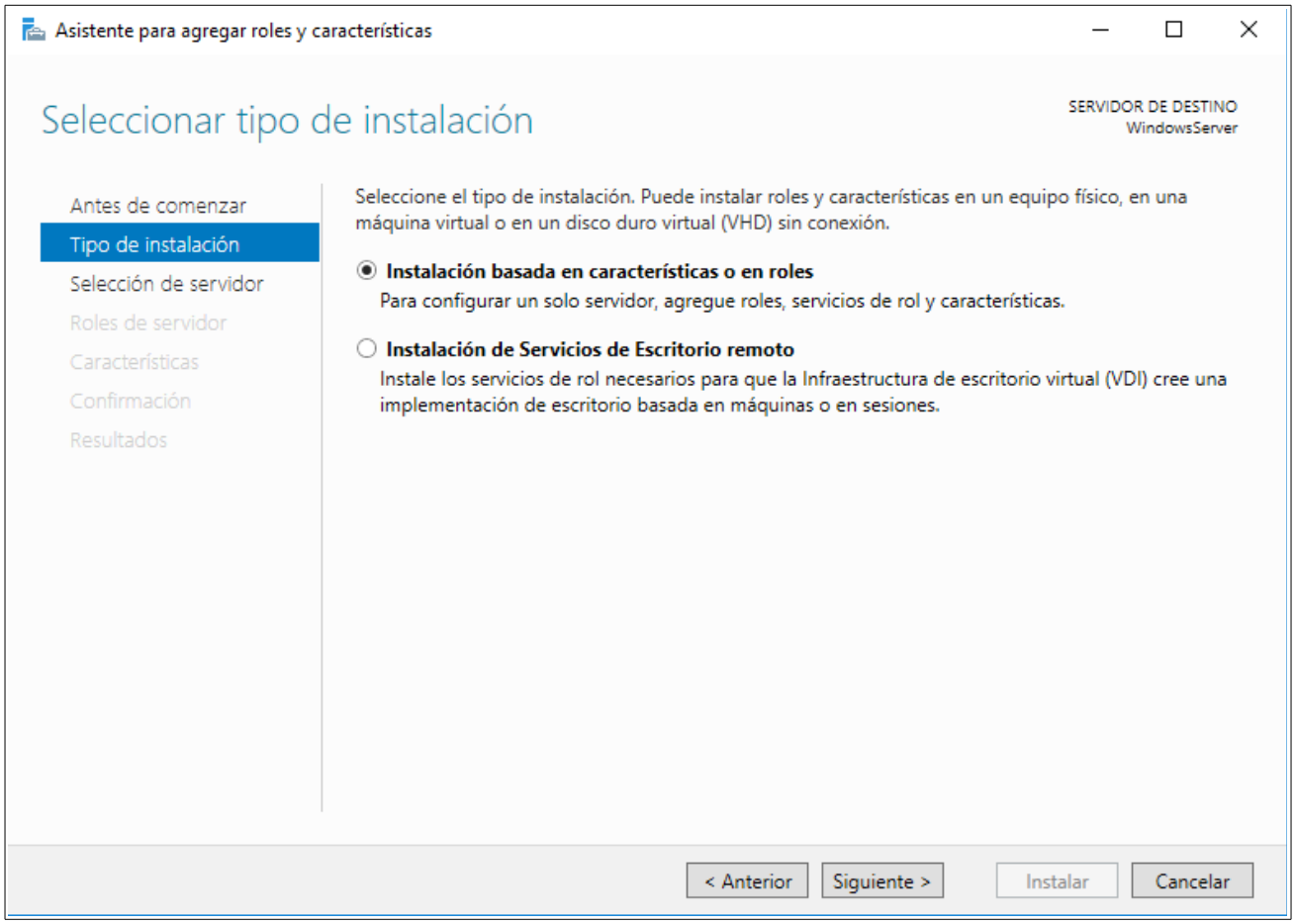

3. On the left, click on ***ADD ROLES AND FEATURES***



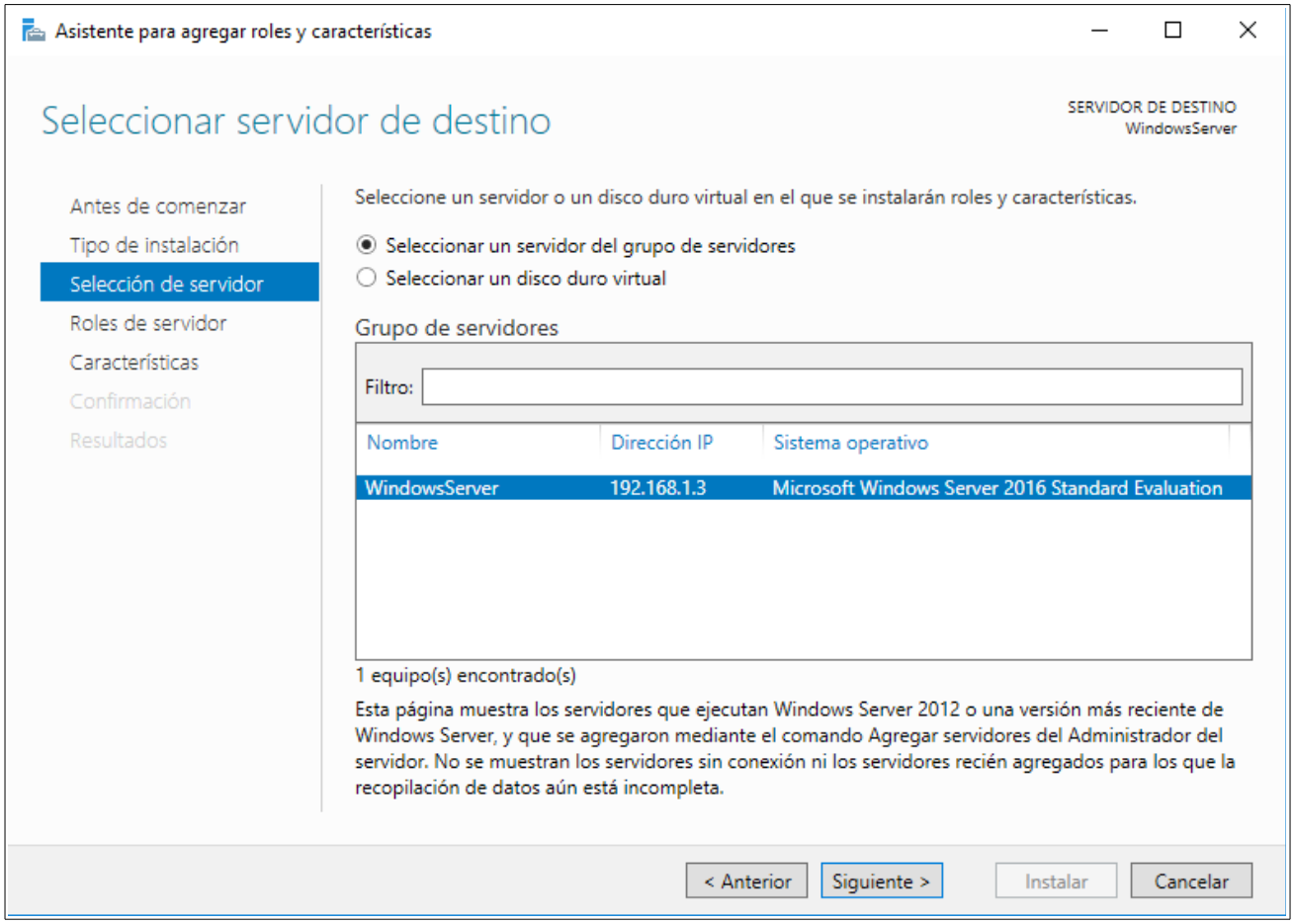

4. Read the information of the wizard and click on ***NEXT***



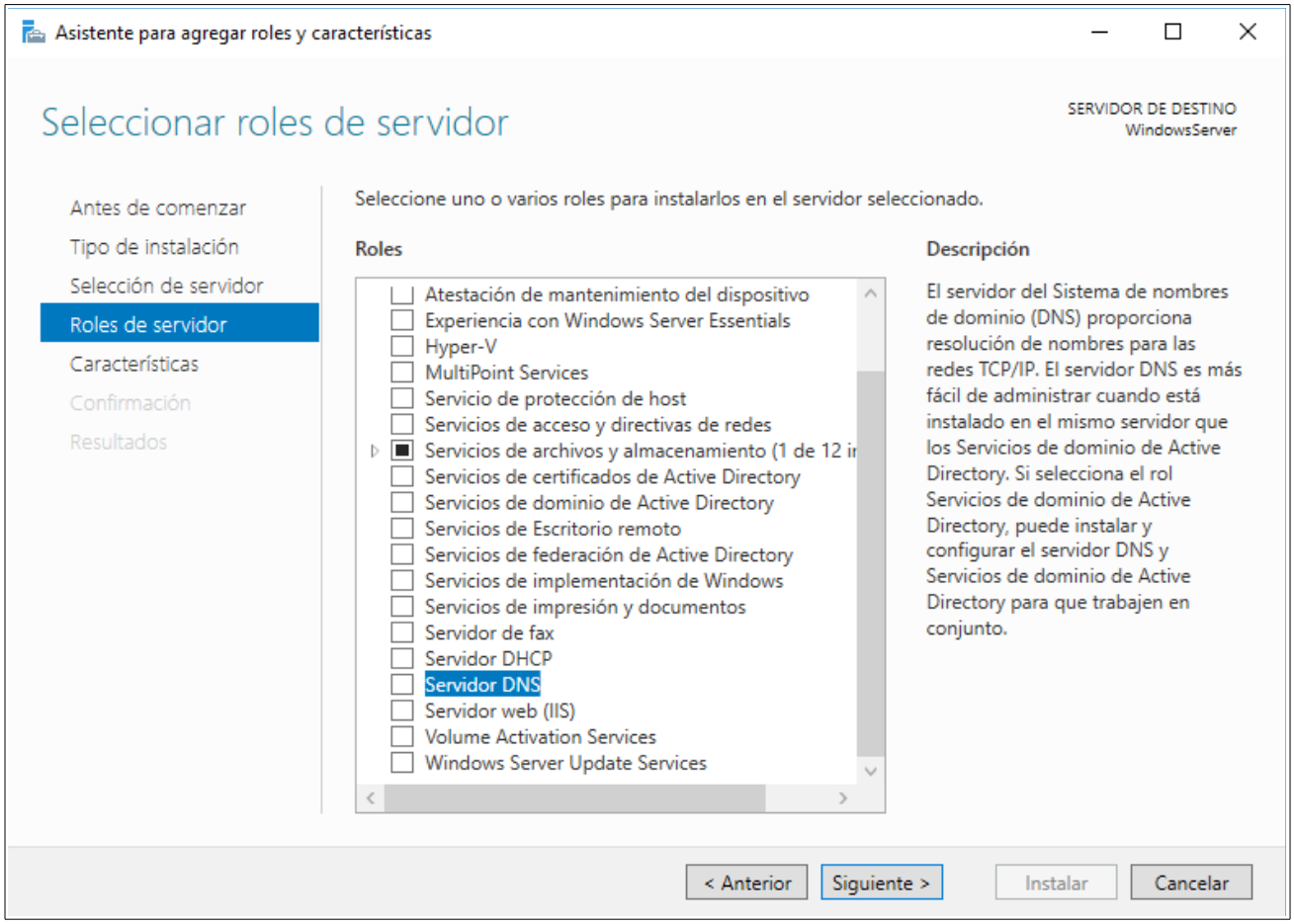
5. Select ***BASIC INSTALLATION*** and click on ***NEXT***



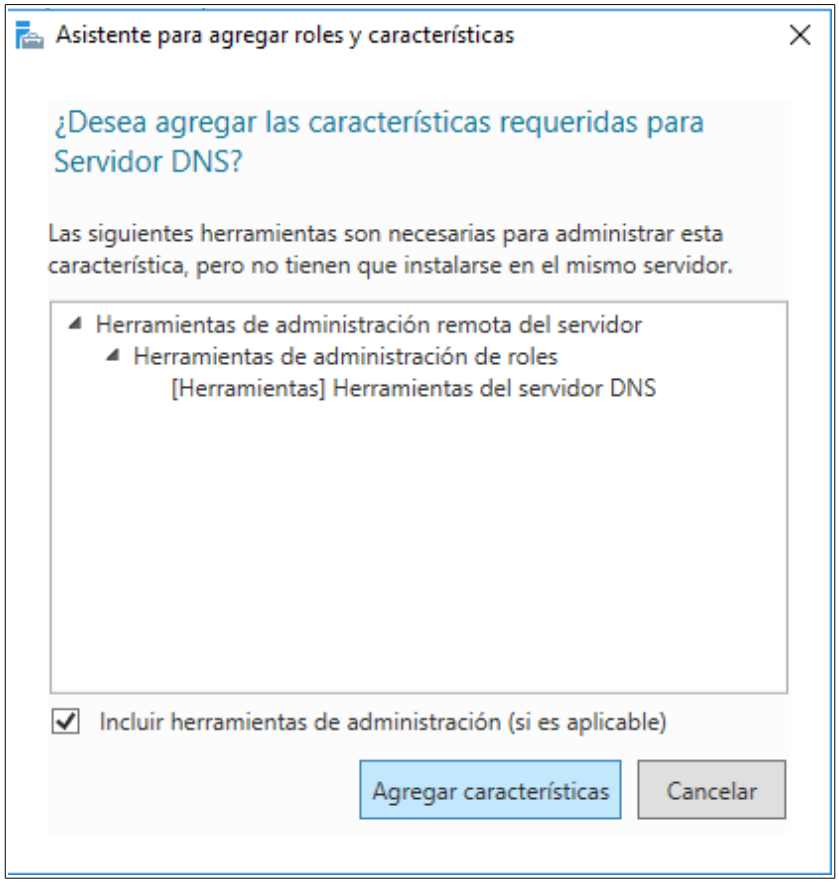

6. Select the server to and click on ***NEXT***



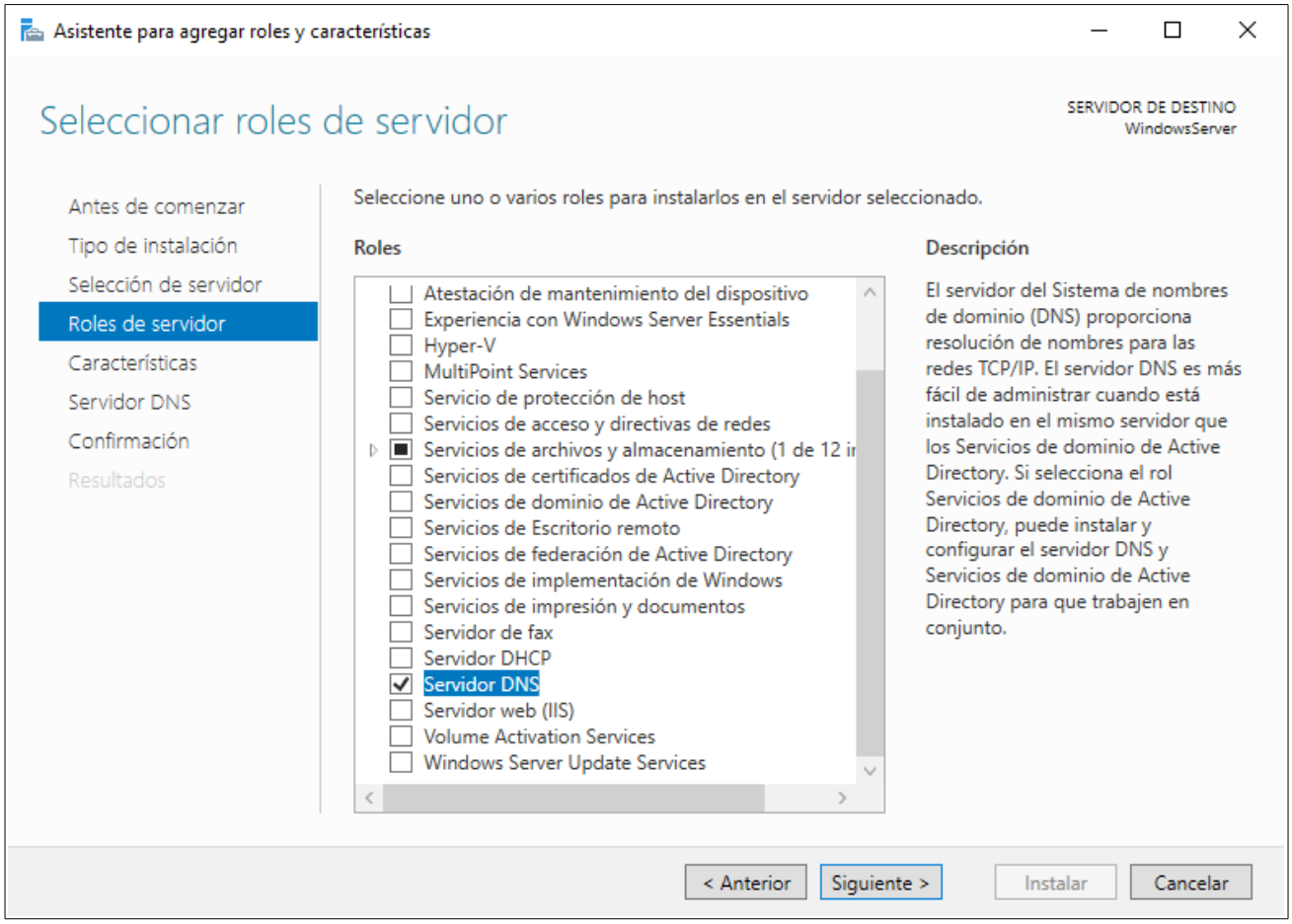

7. Select ***DNS SERVER*** and click on ***NEXT***



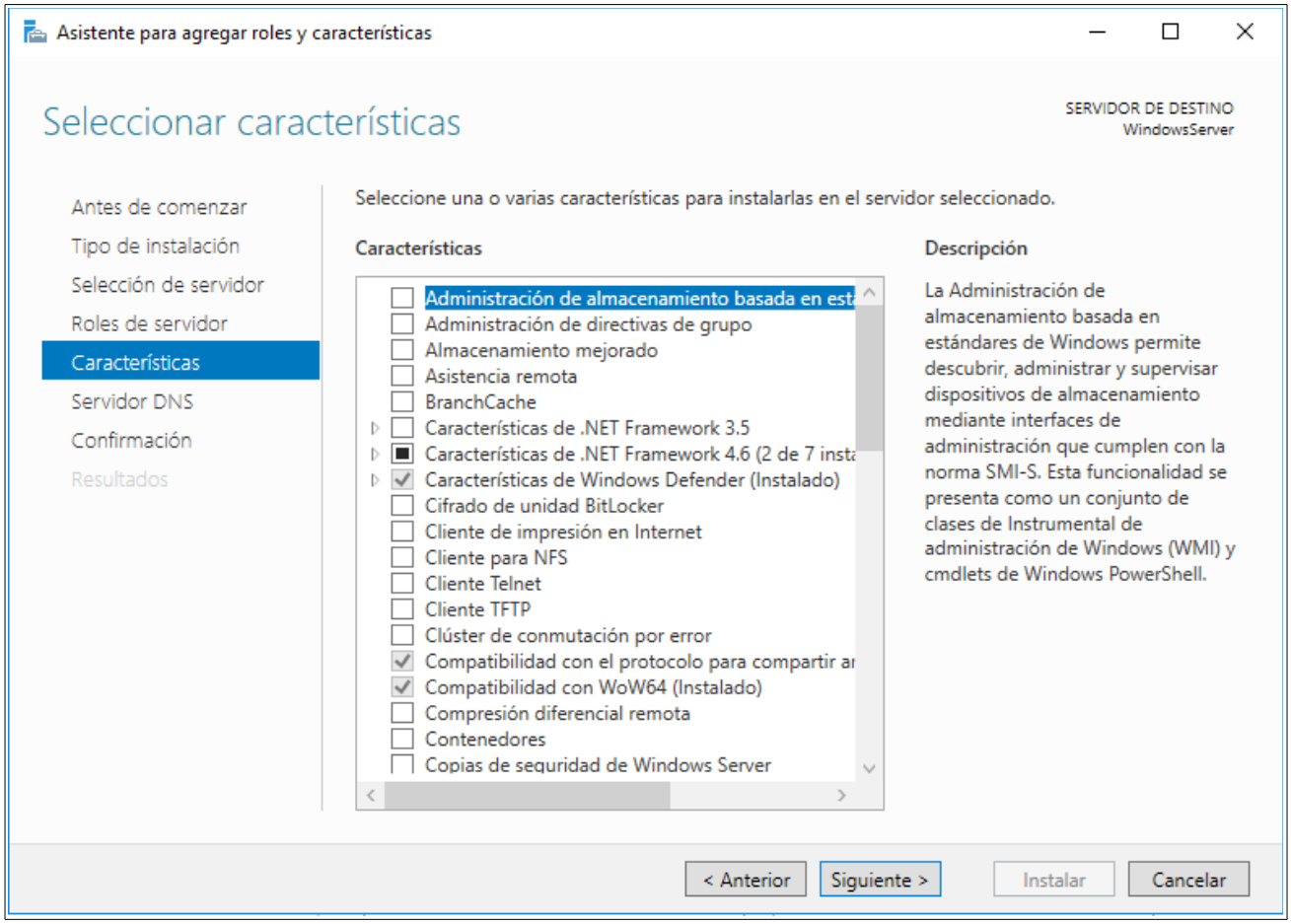

8. Click on ***ADD FEATURES***



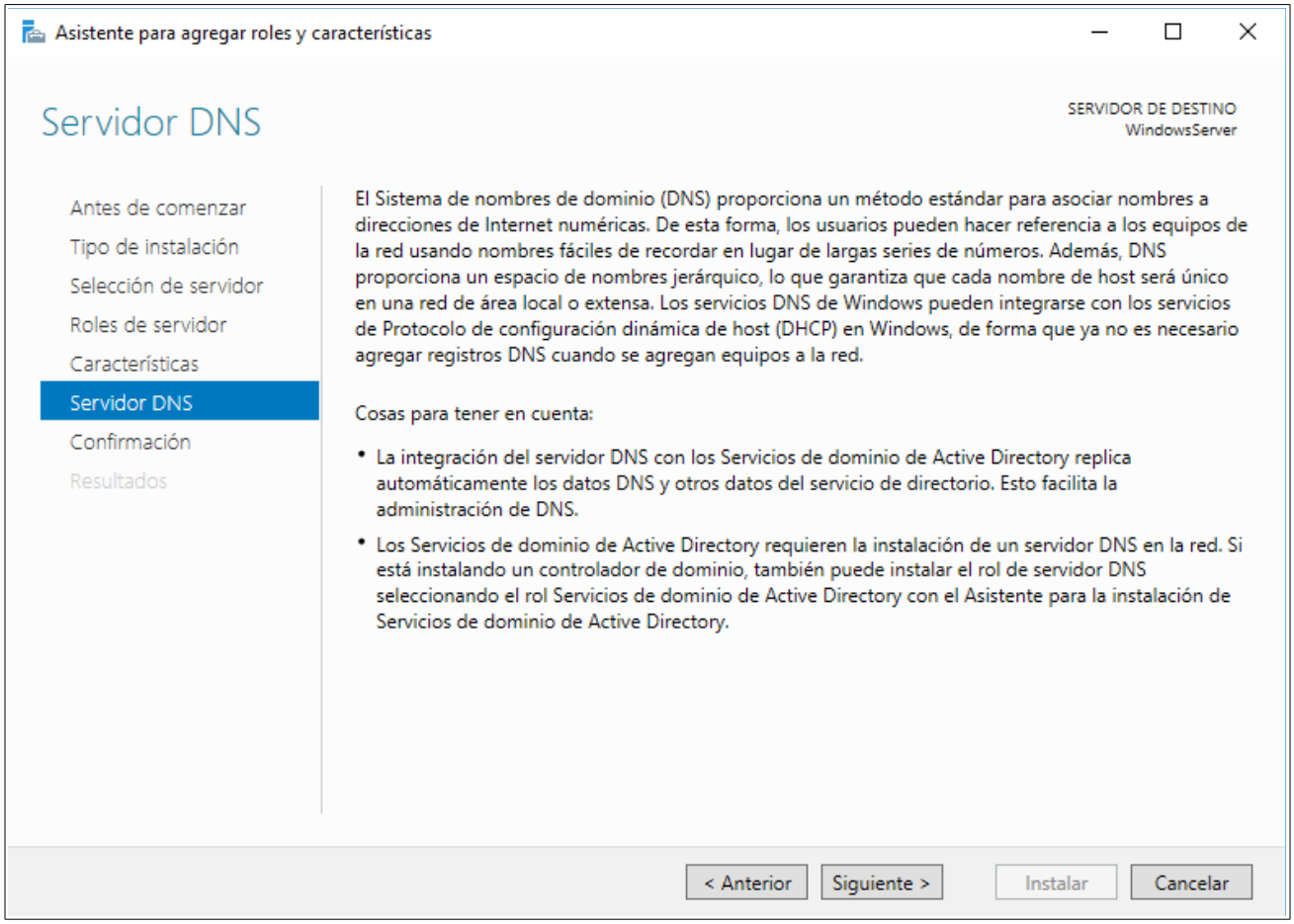

9. Click on ***NEXT***



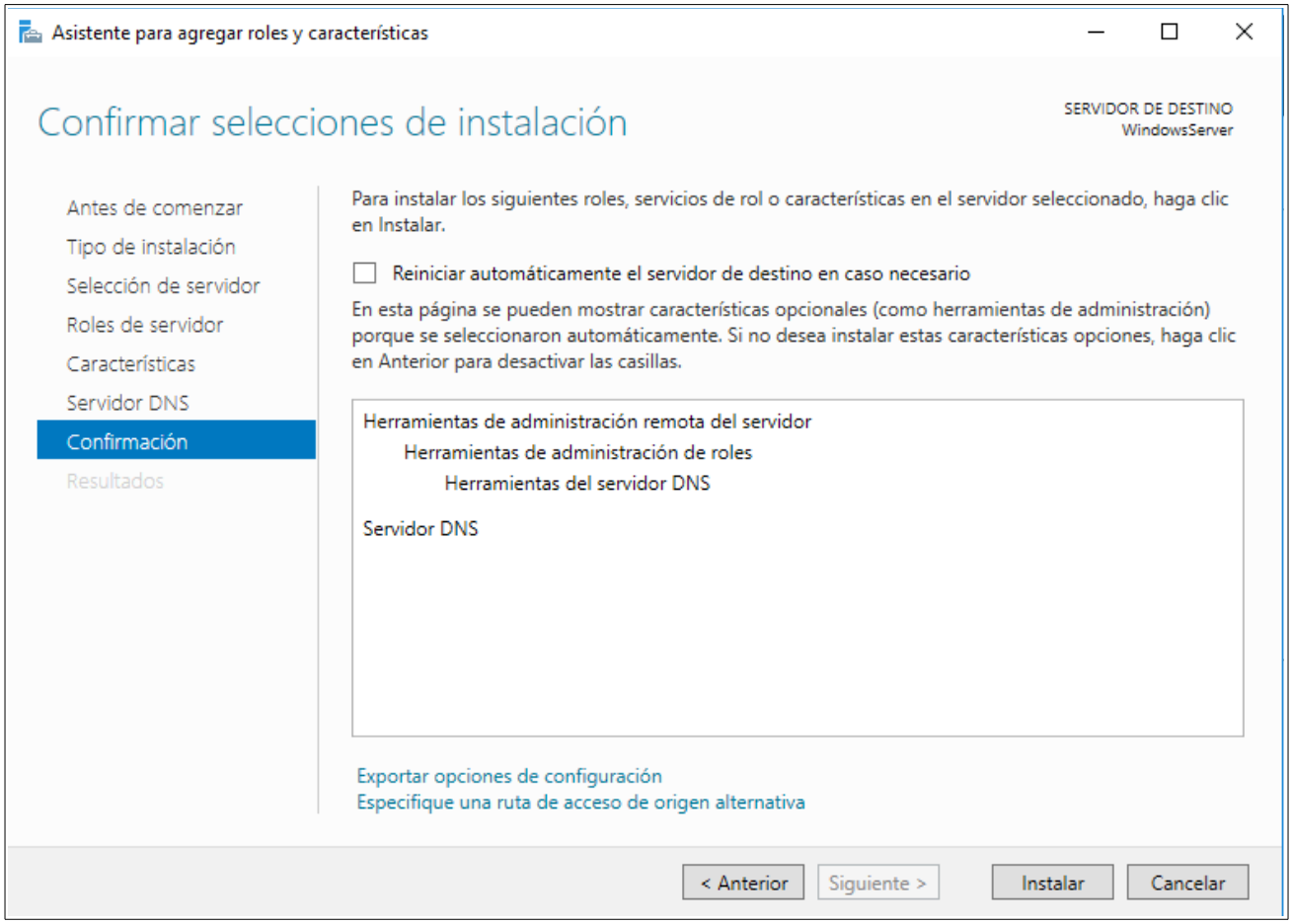

10. We do not want to install any feature so click on ***NEXT***



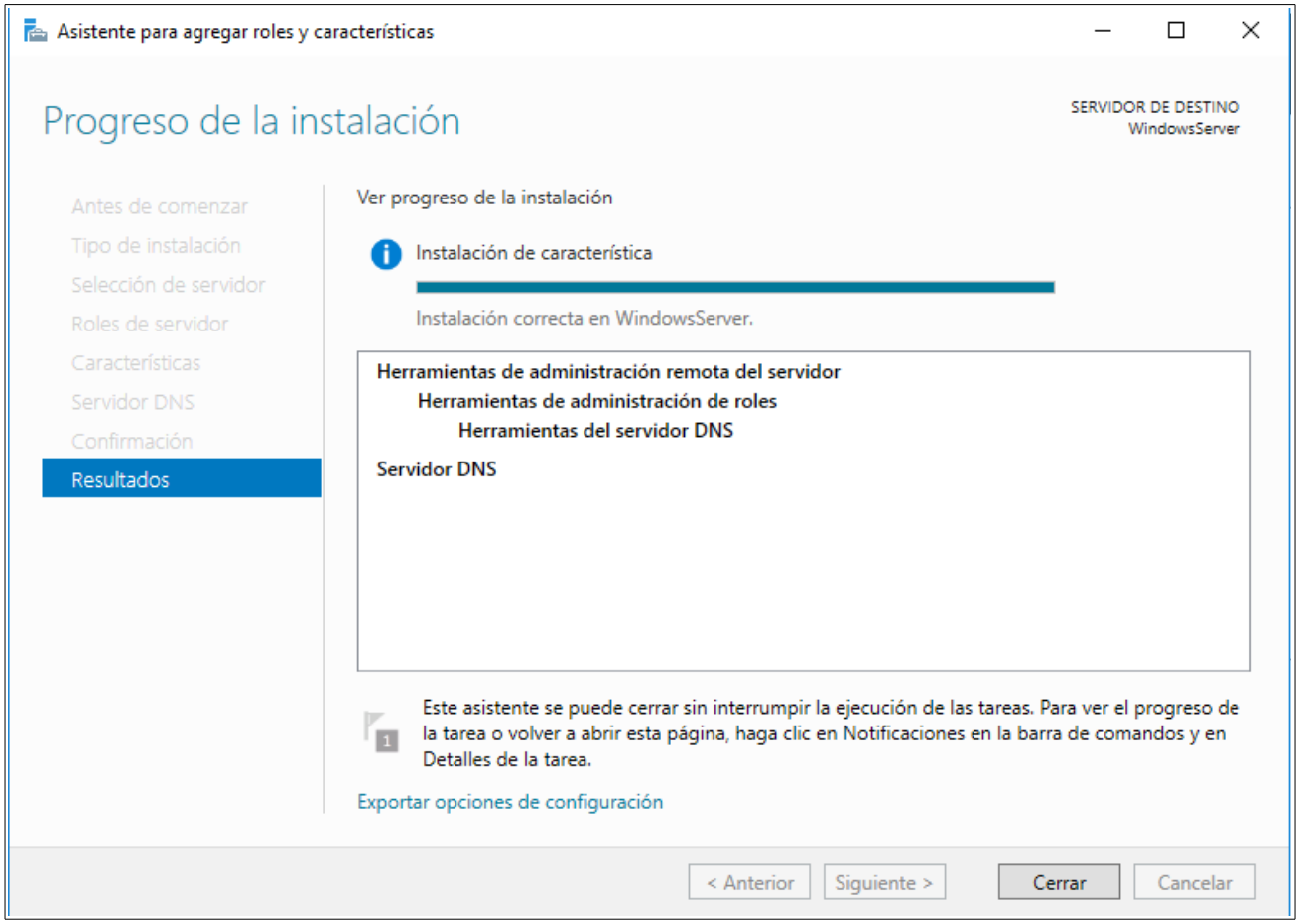

11. Read the information and click on ***NEXT***



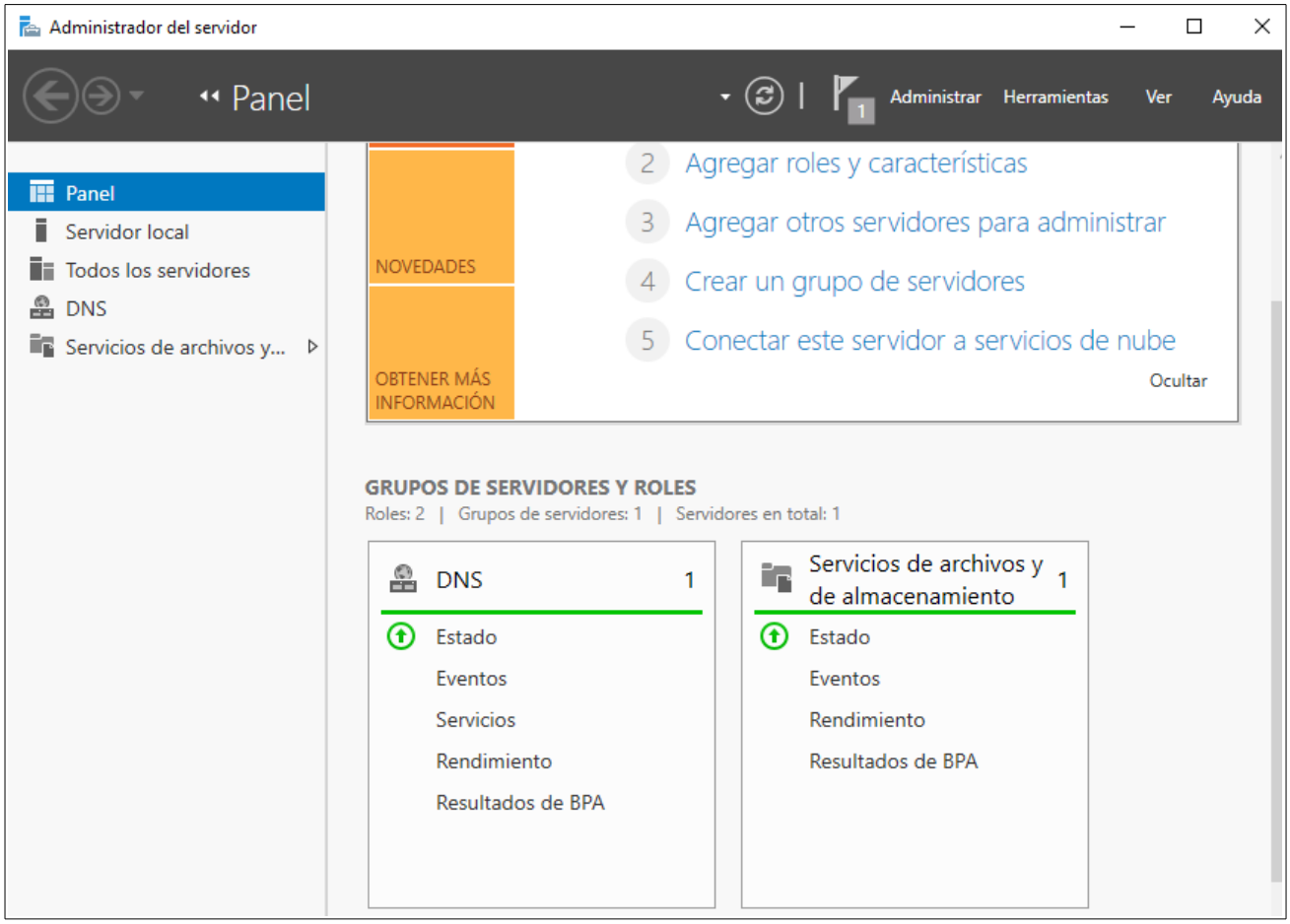

12. Confirm the installation and click on ***INSTALL*** (we can select the automatic reboot)



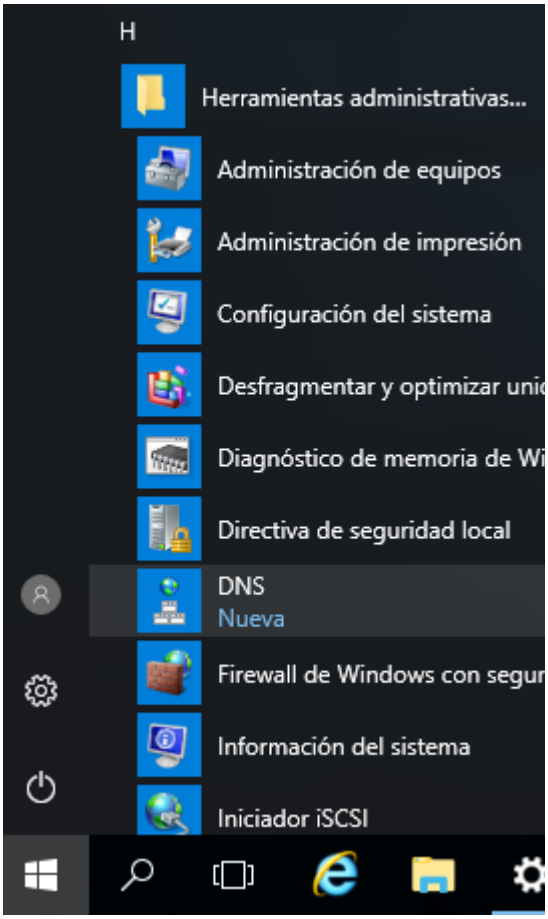

13. And the installation will be completed. Click on ***CLOSE***

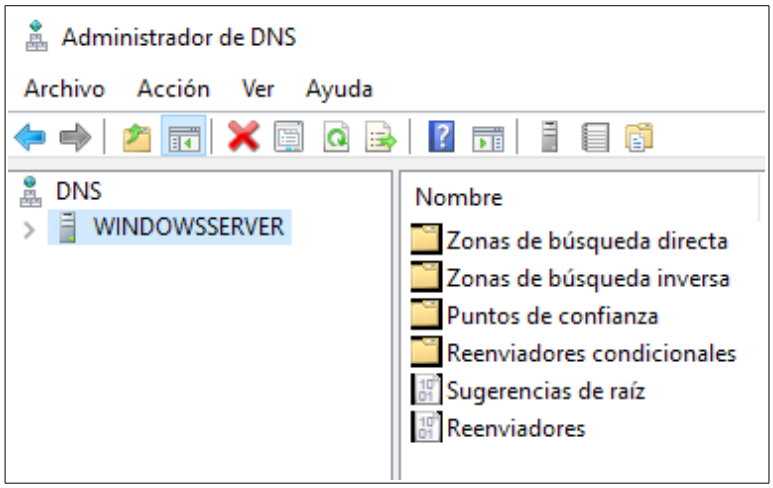



We can see it in the Panel




We can check that the DNS server is installed clicking on ***START MENU > ADMINISTRATIVE TOOLS > DNS***

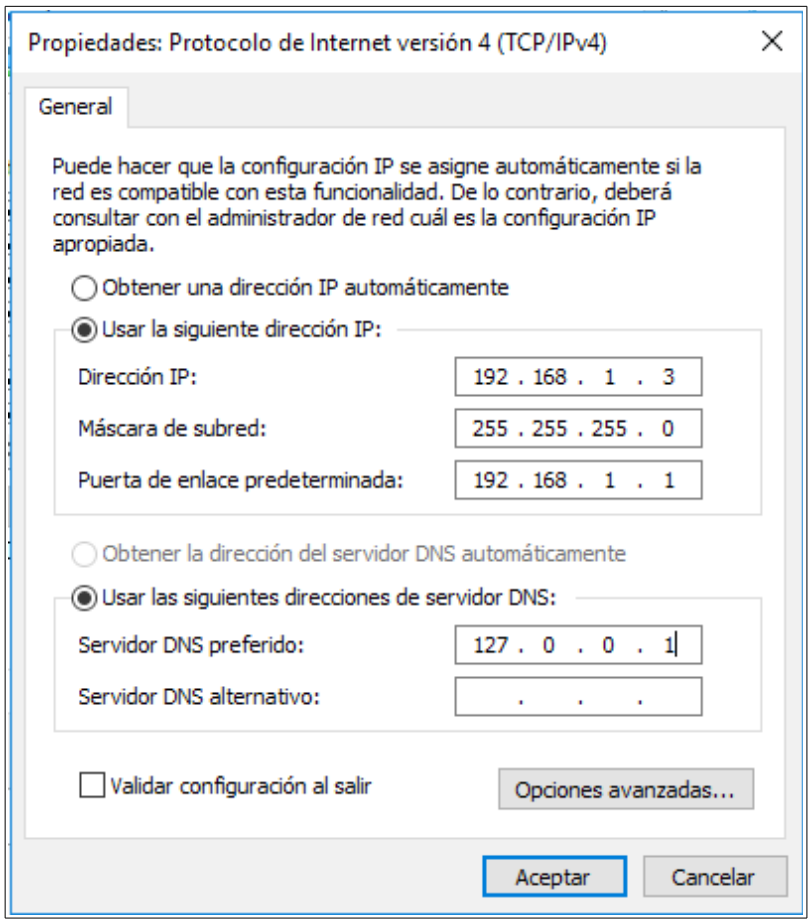

H
Herramientas administrativas...
Administración de equipos
Administración de impresión
Configuración del sistema
Desfragmentar y optimizar uni
Diagnóstico de memoria de Wi
Directiva de seguridad local
DNS
Nueva
Firewall de Windows con segur
Información del sistema
Iniciador iSCSI


Administrador de DNS
Archivo Acción Ver Ayuda
DNS
WINDOWSSERVER
Nombre
Zonas de búsqueda directa
Zonas de búsqueda inversa
Puntos de confianza
Reenviadores condicionales
Sugerencias de raíz
Reenviadores

### 2.1.2 Configuring the DNS server

By default, the server is configured as only-cache, it is not authorized in any zone.

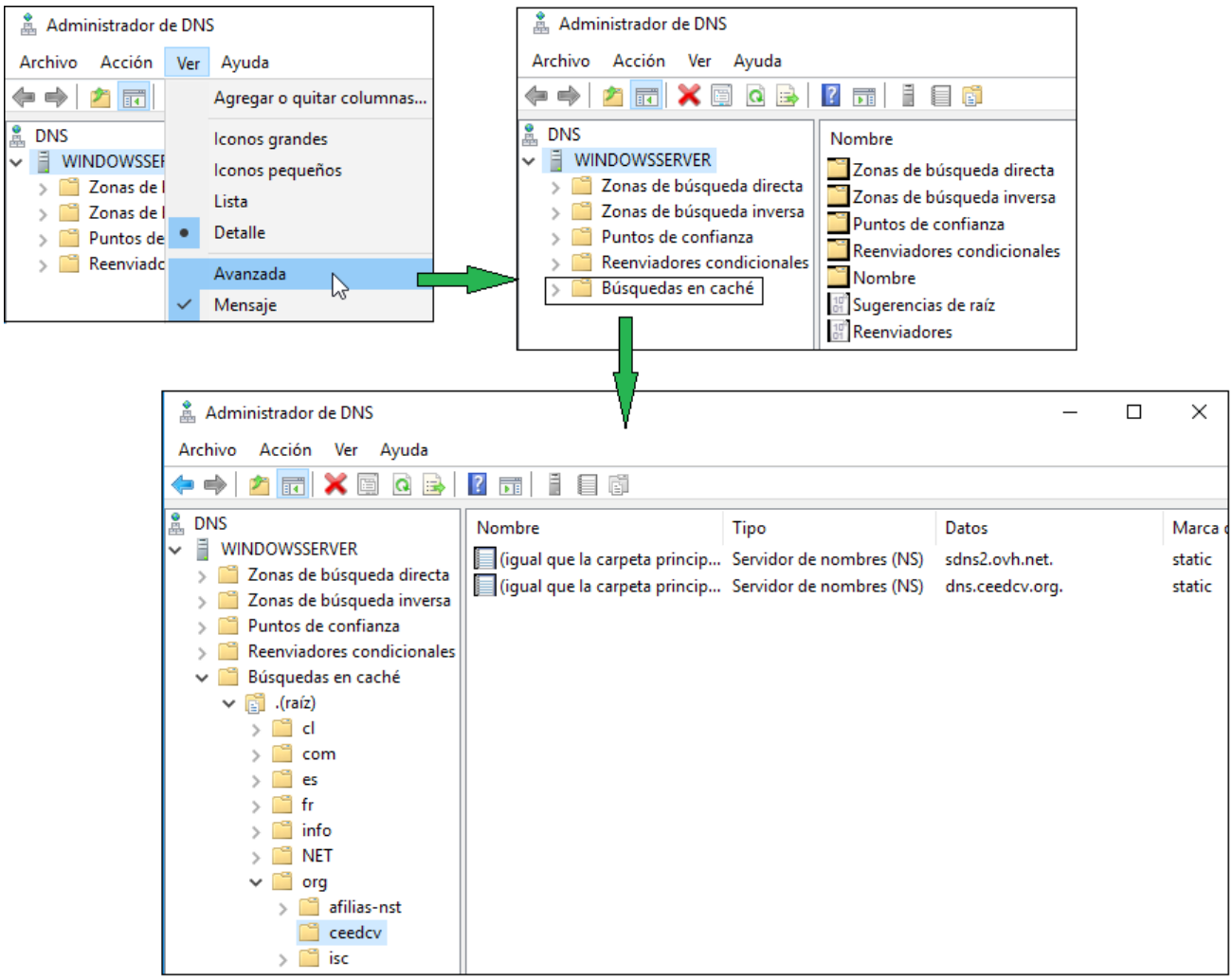
To check if the server can resolve domain names from Internet, we are going to change the DNS server from the network configuration and use the **loopback** address (127.0.0.1):




Then we will use the nslookup command to resolve a name, for instance *www.ceedcv.org*:

```
C:\Windows\system32>nslookup www.ceedcv.org
Servidor:  localhost
Address:  127.0.0.1

Respuesta no autoritativa:
Nombre:  www.ceedcv.org
Address:  51.254.244.219
```

We can see the server cache and information about the domain we have consulted. For that, we have to go to the DNS administrator window and click on ***VIEW > ADVANCED***




## 2.2 Configuring DNS server in WS2016 (primary, forward lookup zone)

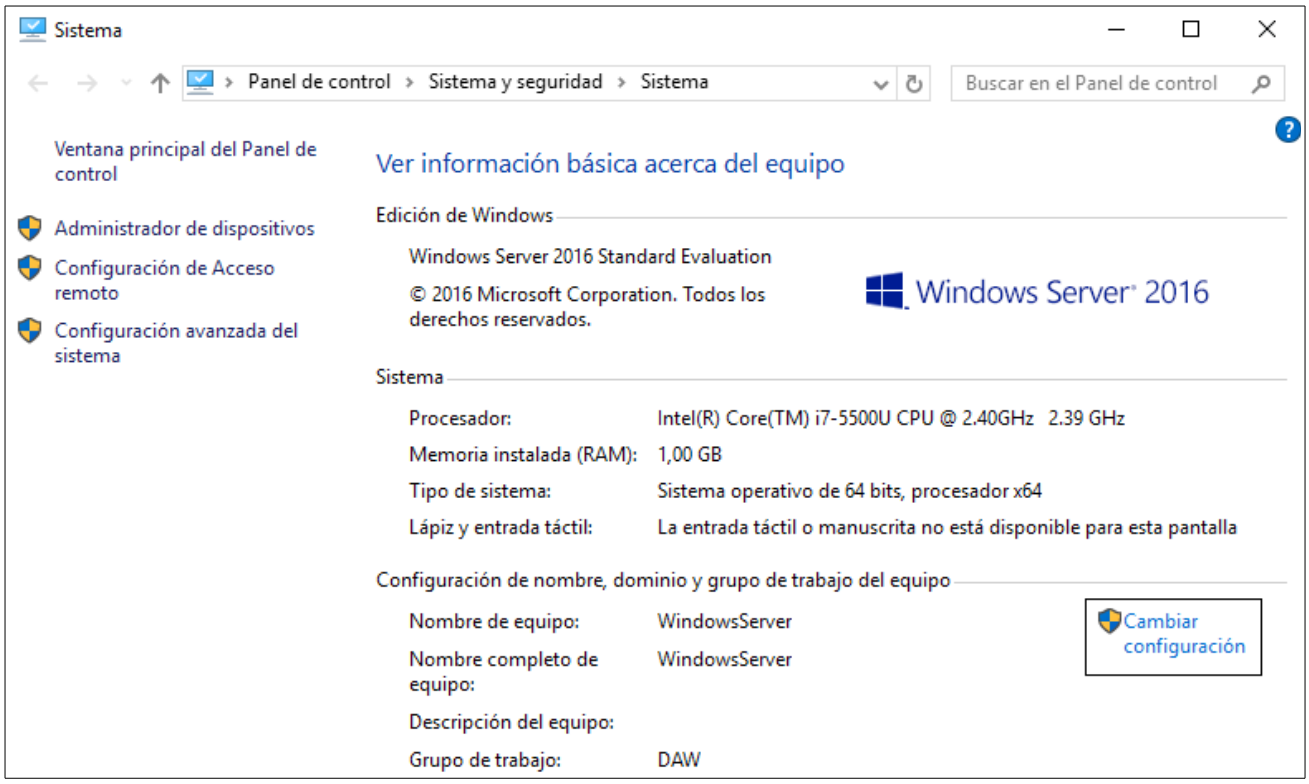
Now we are going to configure the DNS server as primary to a forward lookup zone, so in this case:

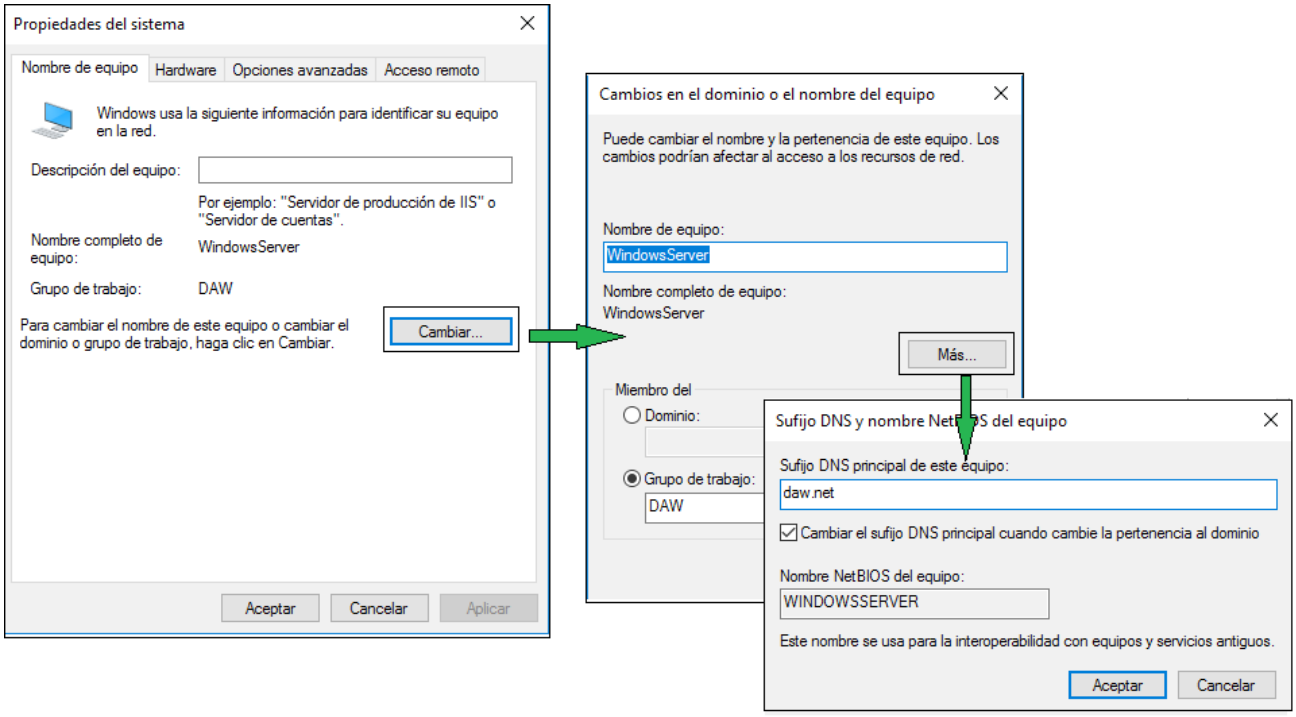
- The server will only works to the local network (not to hosts from Internet)
- The server will works as master (primary) and it will have authority to the domain *daw.net*:

- Dynamic updates will be forbidden.
- The DNS server domain will be *windowsserver.daw.net* (***NS record***)
- The following domain names will be configured (***A record***):
  - *linuxclient.daw.net* associated to the IP address 192.168.1.4
  - *linuxserver.daw.net* associated to the IP address 192.168.1.2
  - *windowsserver.daw.net* associated to the IP address 192.168.1.3
- The following aliases will be configured (***CNAME record***):
  - *ns.daw.net* will be an alias of *windowsserver.daw.net*
  - *slinux* will be an alias of *linuxserver.daw.net*
  - *swindows* will be an alias of *windowsserver.daw.net*
  - *client* will be an alias of *linuxclient.daw.net*

### 2.2.1 Configuring the DNS suffix

First, we are going to give a suffix (*daw.net*) to our server. For that, we have to go to ***START MENU(RIGHT BUTTON) > SYSTEM > CHANGE CONFIGURATION > CHANGE > MORE***

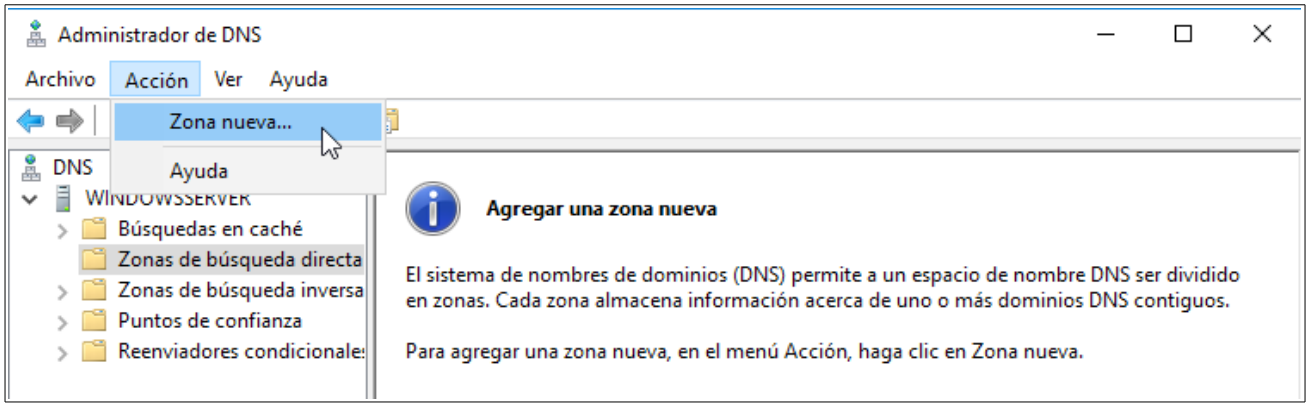




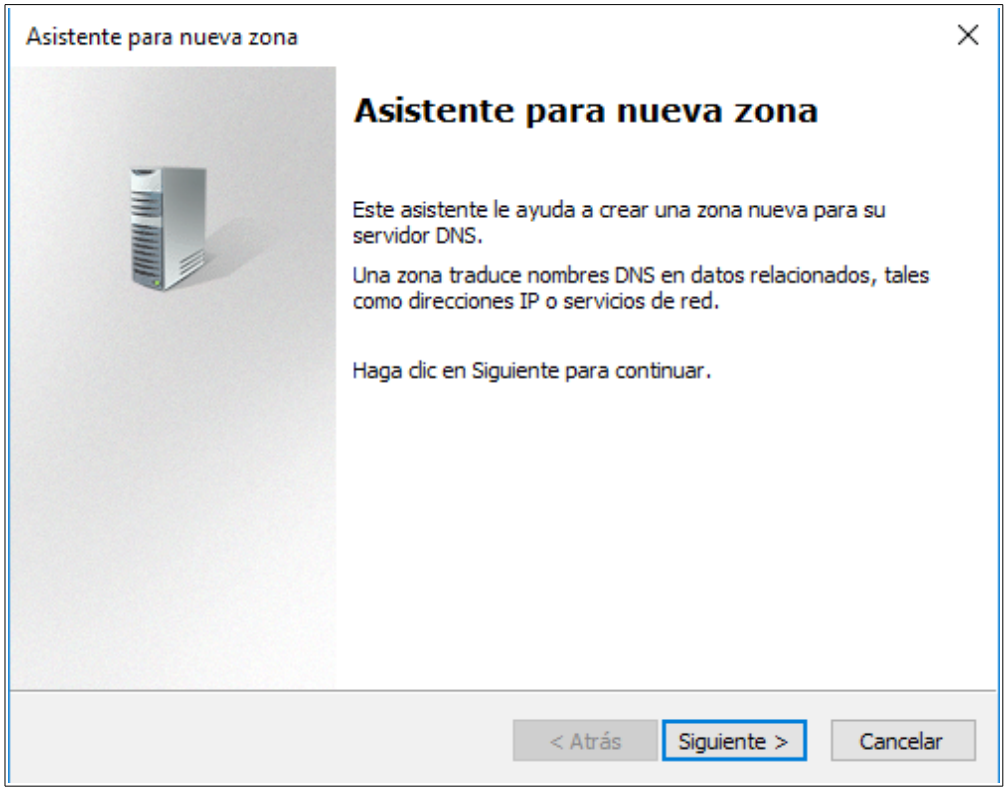

### 2.2.2 Configuring the forward lookup zone

For configure the forward zone you have to follow the next steps:

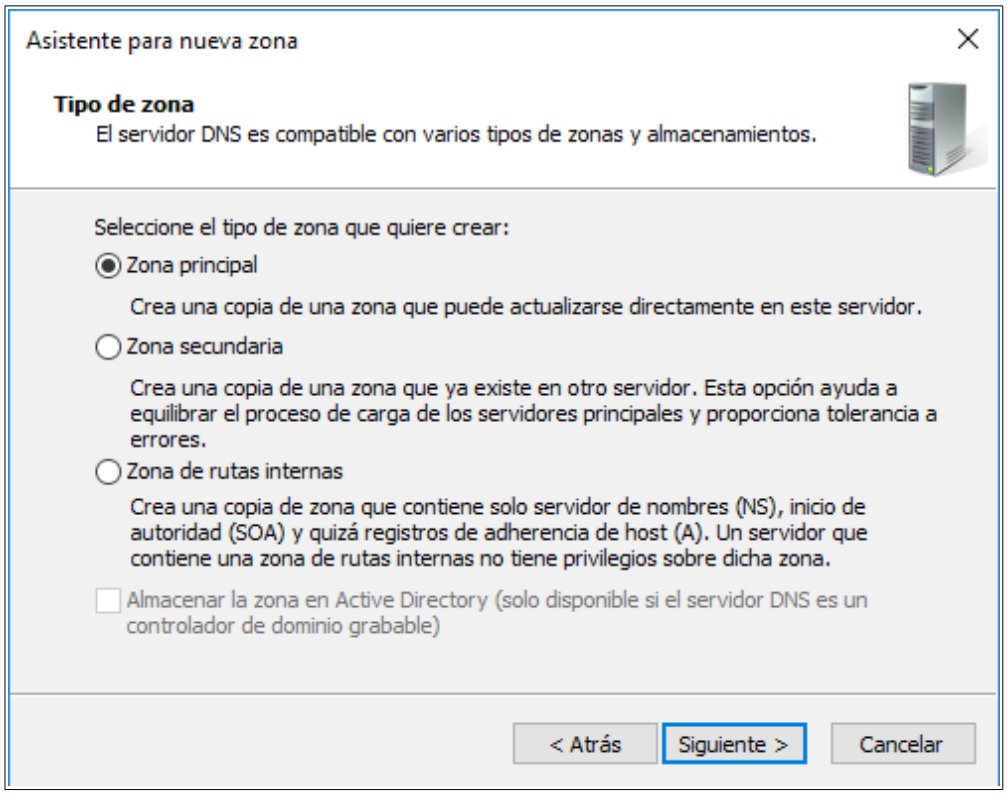
1. Go to the server administration window, select ***FORWARD LOOKUP ZONE*** and click on ***ACTION*** and ***NEW ZONE***



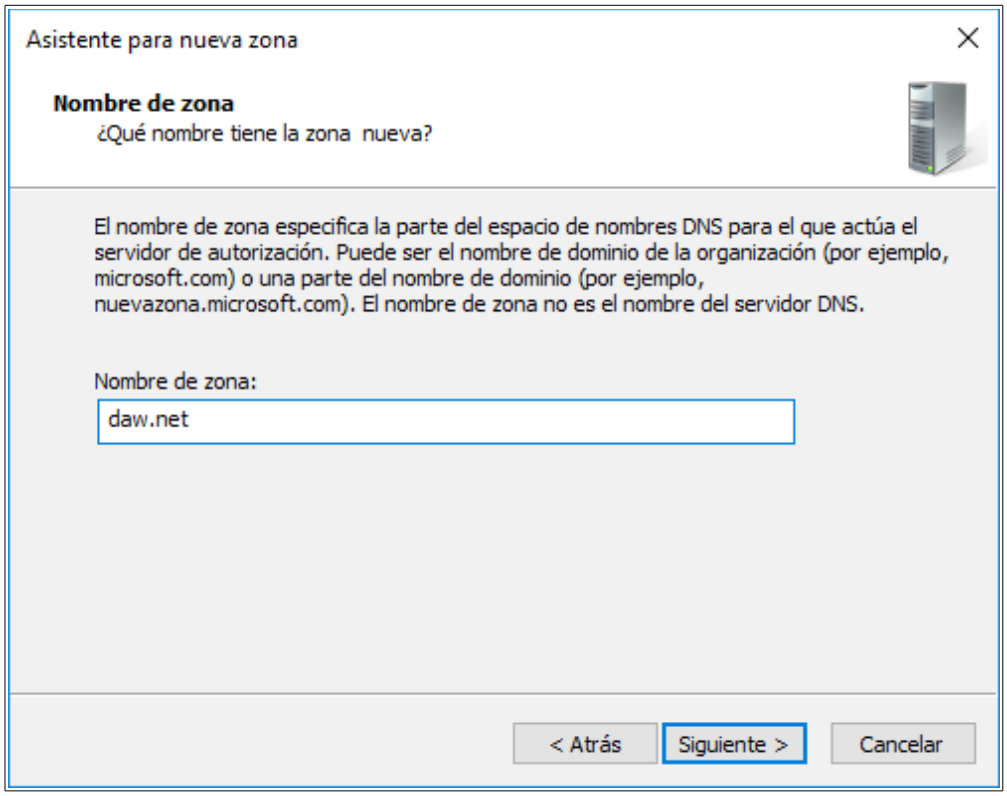

2. Read the information of the wizard and click on ***NEXT***



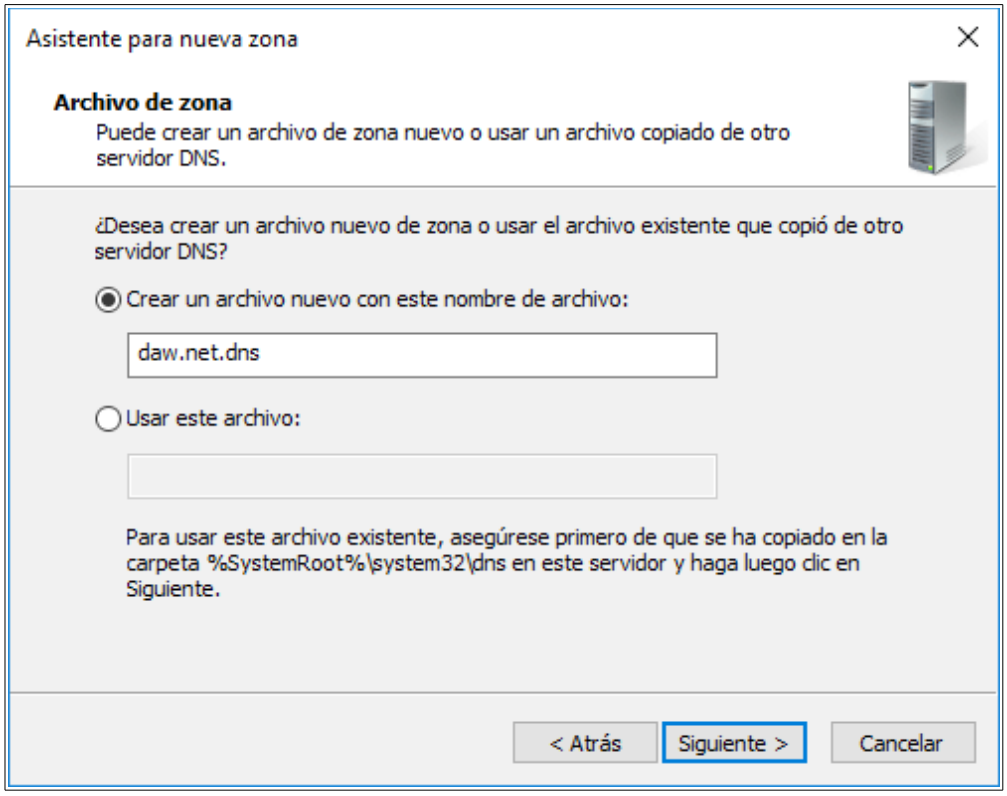

3. Select ***PRIMARY ZONE*** and click on ***NEXT***



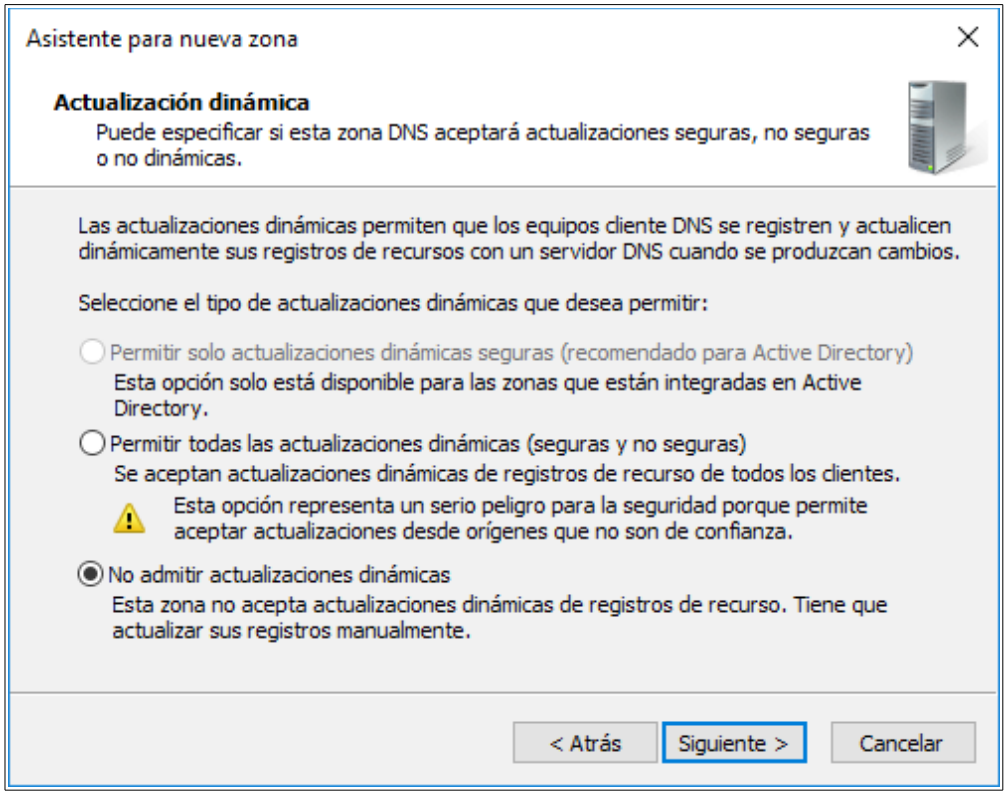
4. Write *daw.net* as the name of the zone and click on ***NEXT***



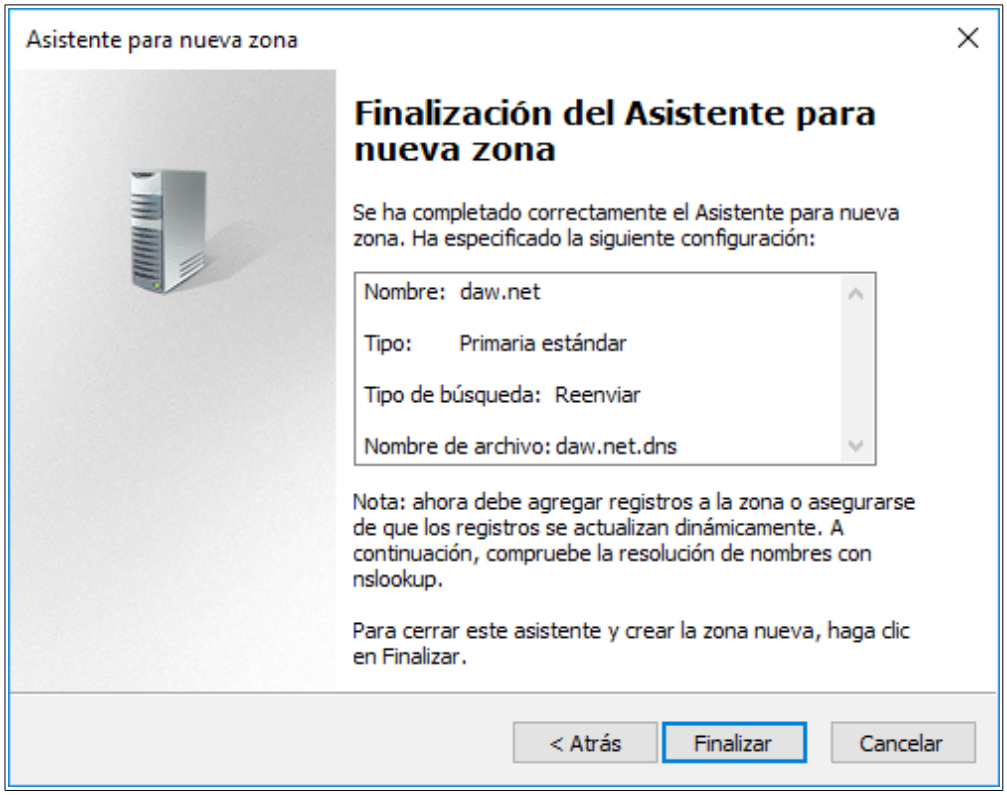

5. Select the option of ***CREATE A NEW FILE WITH THIS FILE NAME*** and click on ***NEXT***



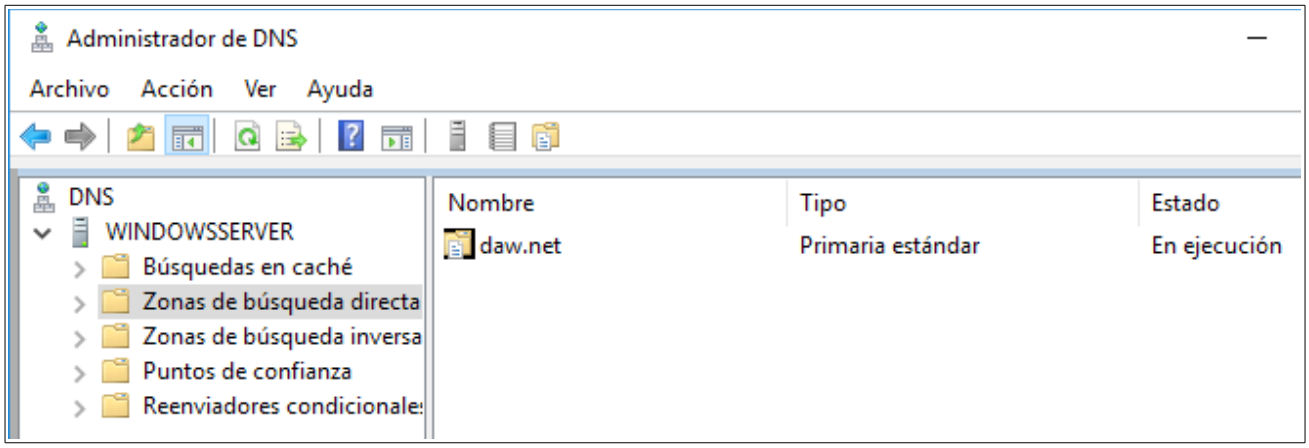

6. Select the option of ***DO NOT ALLOW DYNAMIC UPDATES*** and click on ***NEXT***



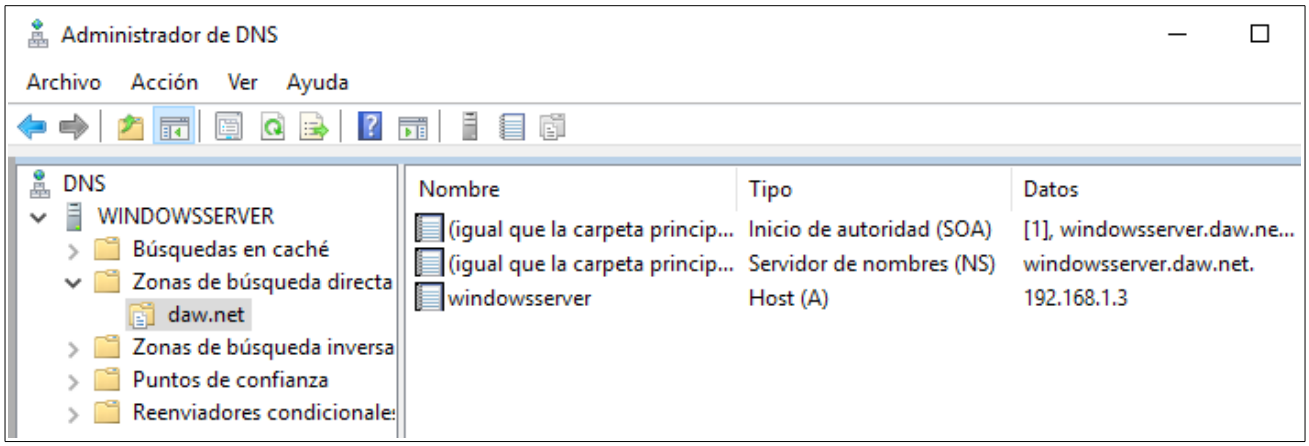

7. Read the summary and click on ***FINISH***



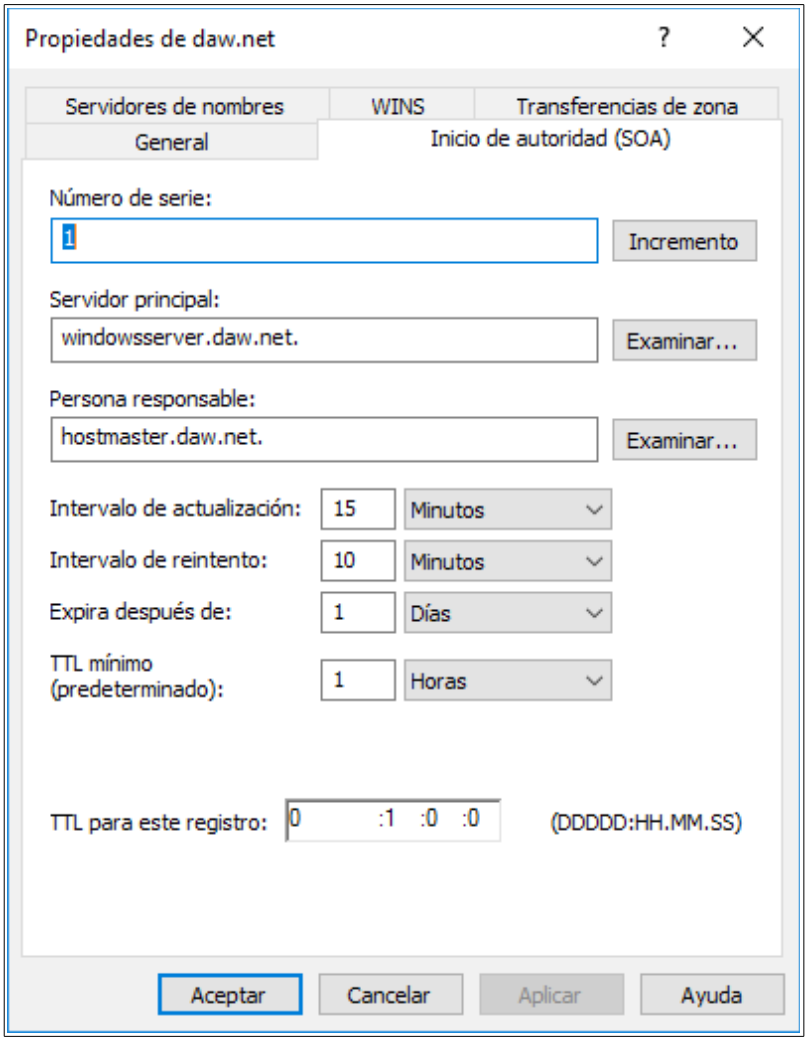
You can see that there is new entry in ***FORWARD LOOKUP ZONES***



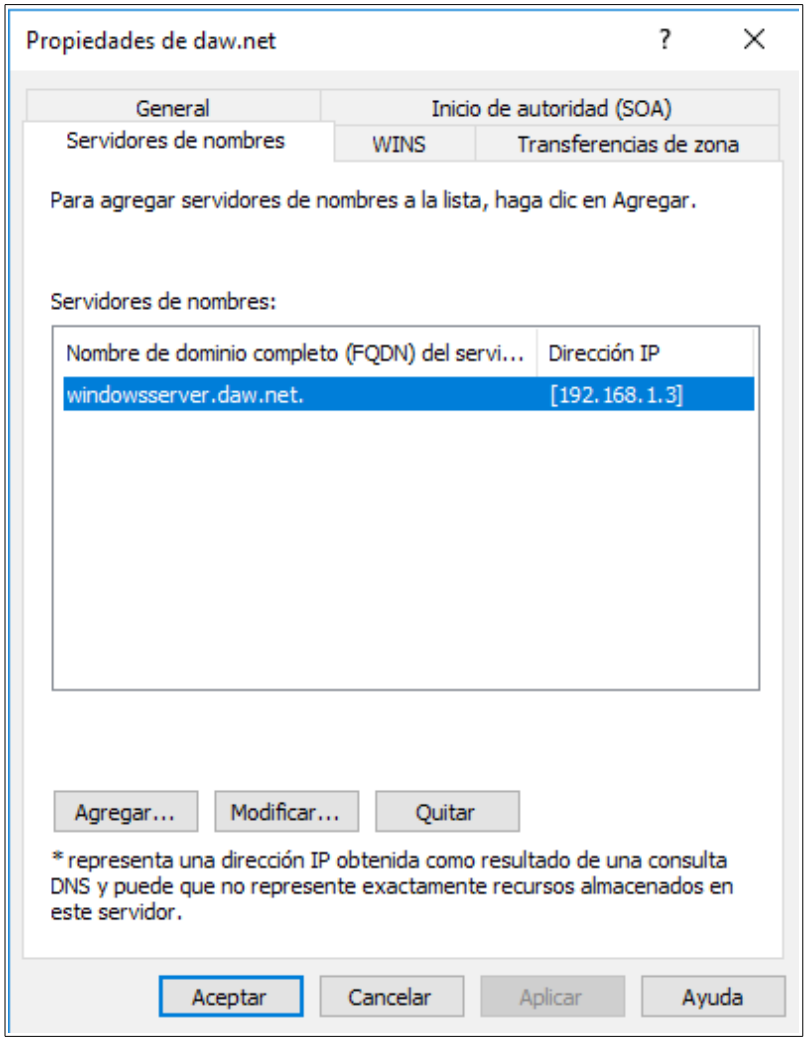

8. Click twice on *daw.net* and you will see the ***SOA*** and ***NS*** records.

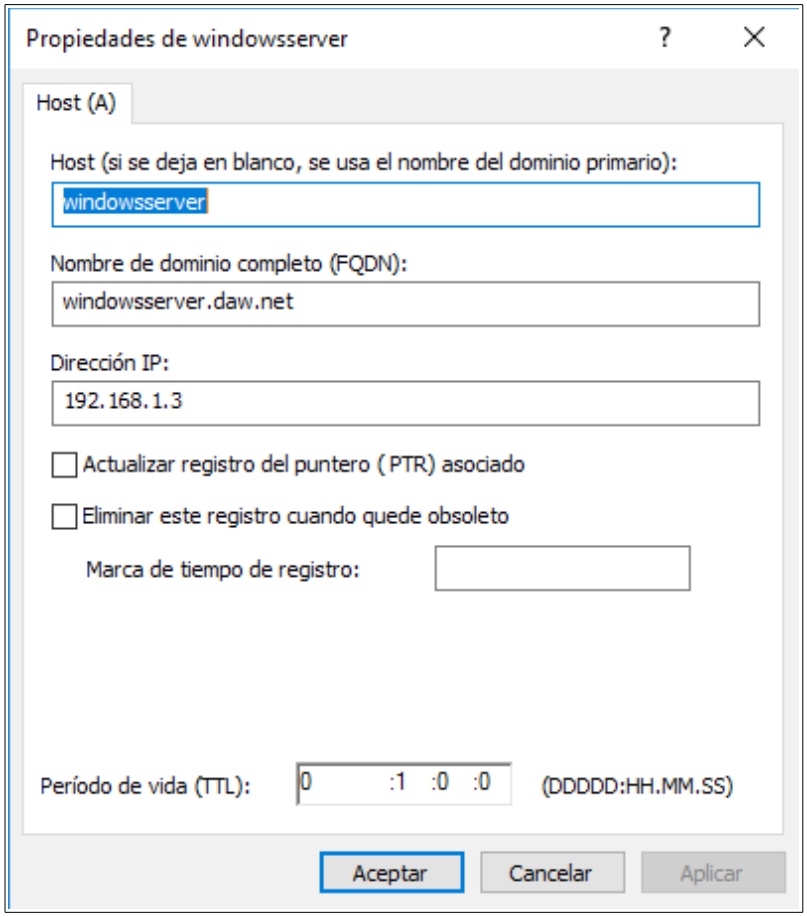



9. Click twice on the ***SOA*** record and see its properties.



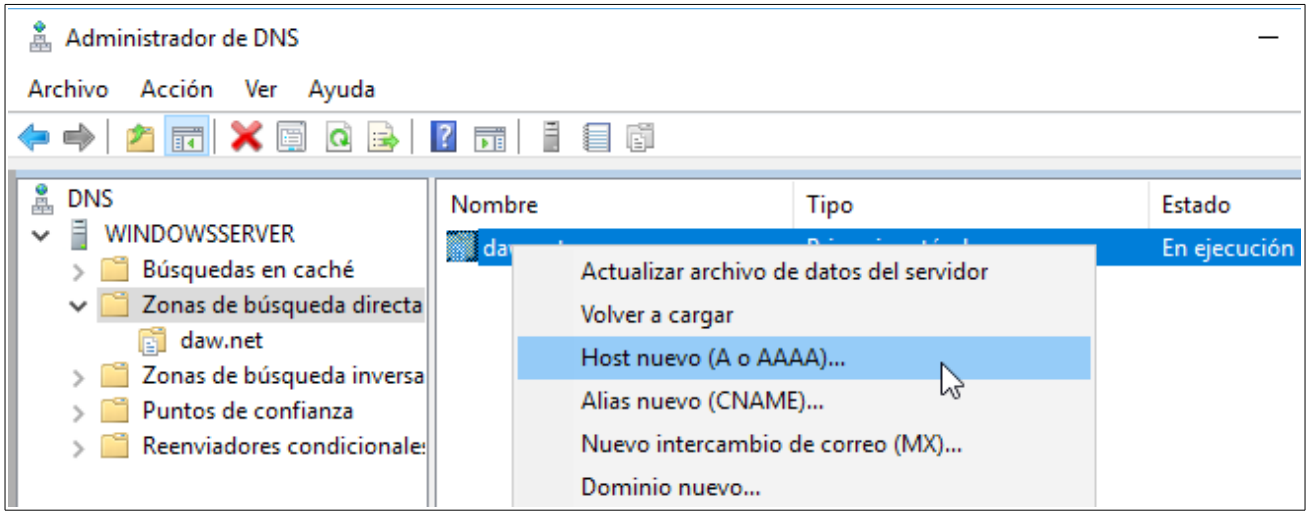

10. Click twice on the ***NS*** record and the ***A*** record to see their properties.


Propiedades de daw.net
General
Inicio de autoridad (SOA)
Servidores de nombres
WINS
Transferencias de zona
Para agregar servidores de nombres a la lista, haga clic en Agregar.
Servidores de nombres:
Nombre de dominio completo (FQDN) del servi...
Dirección IP
windowsserver.daw.net.
[192.168.1.3]
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.
Aceptar
Cancelar
Aplicar
Ayuda

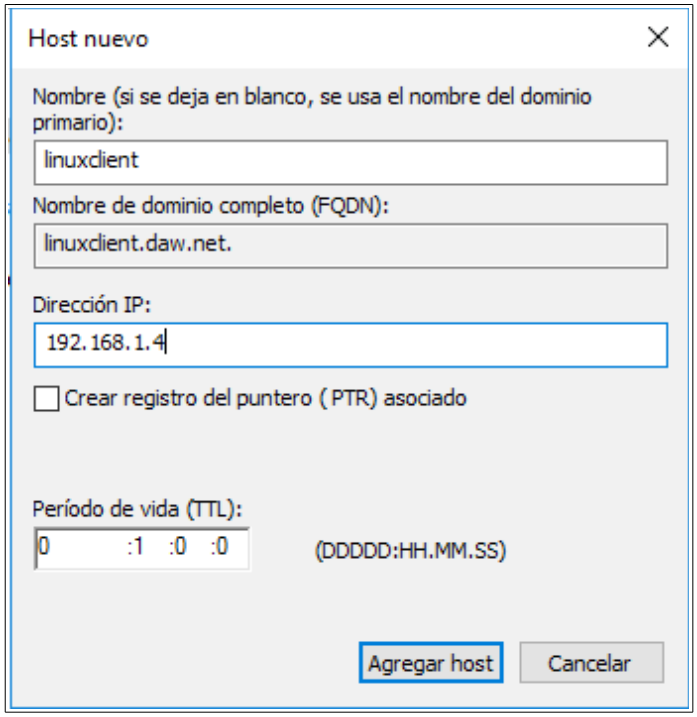


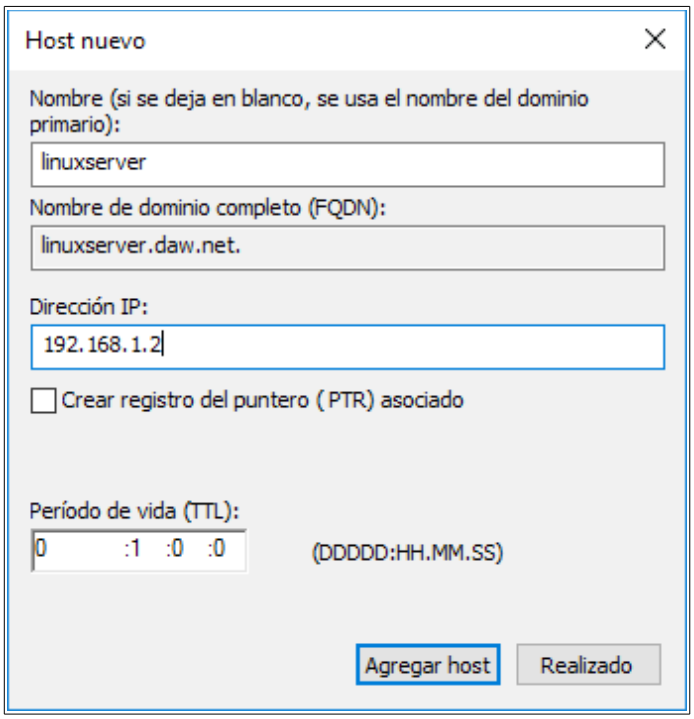

Now we are going to create the A records for the other two virtual machines.

11. Click with the right button on *daw.net* and click on ***NEW HOST (A or AAAA)***



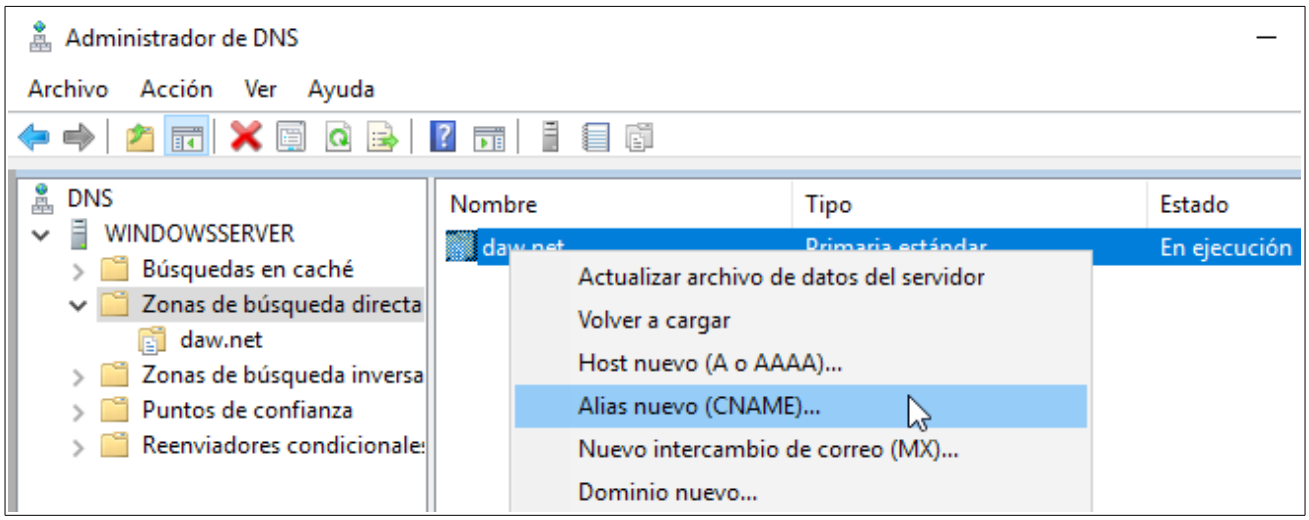
12. Write the name and the IP address for each machine



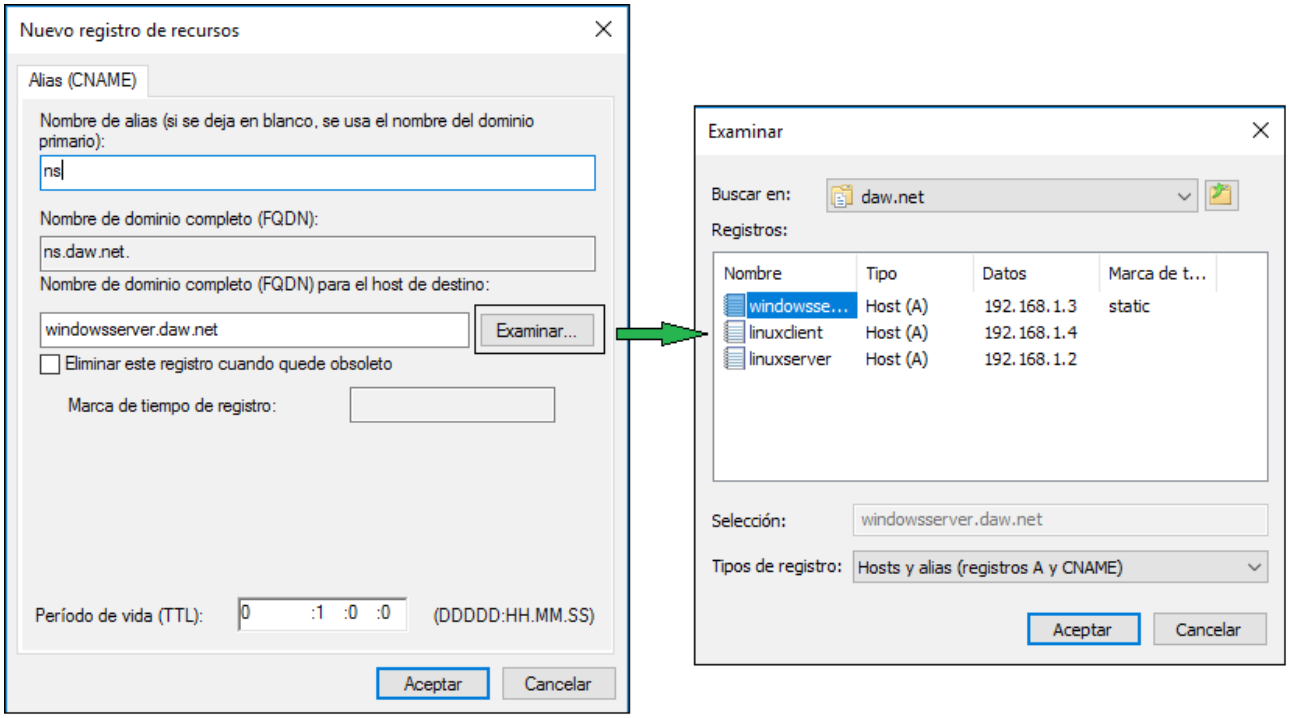



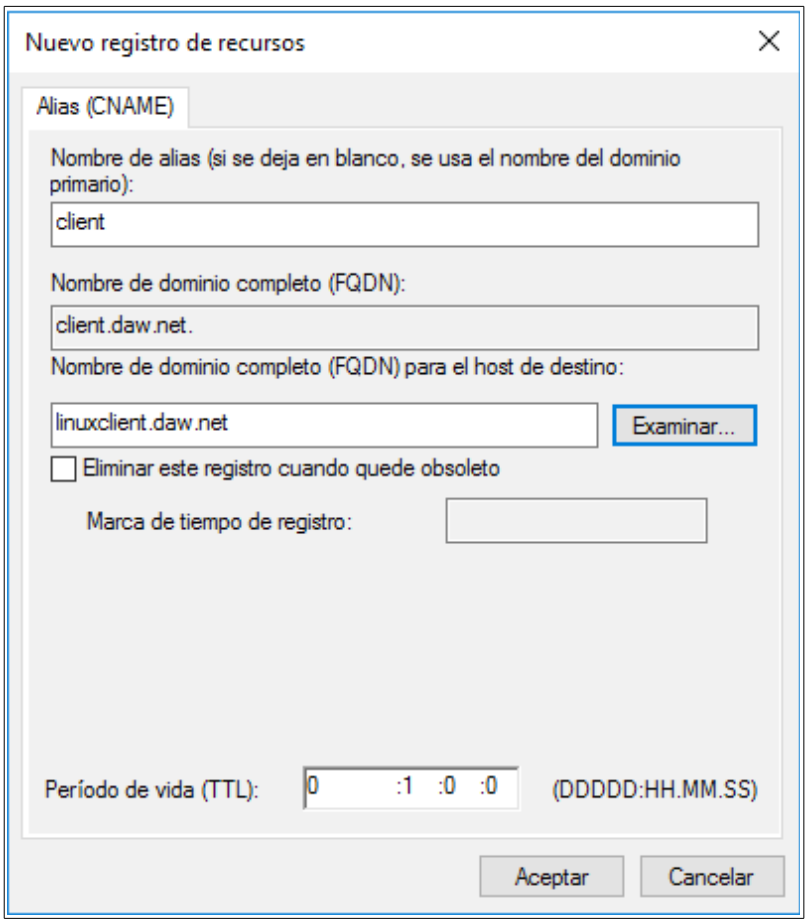
Finally we are going to create the ***CNAME*** records to the aliases.

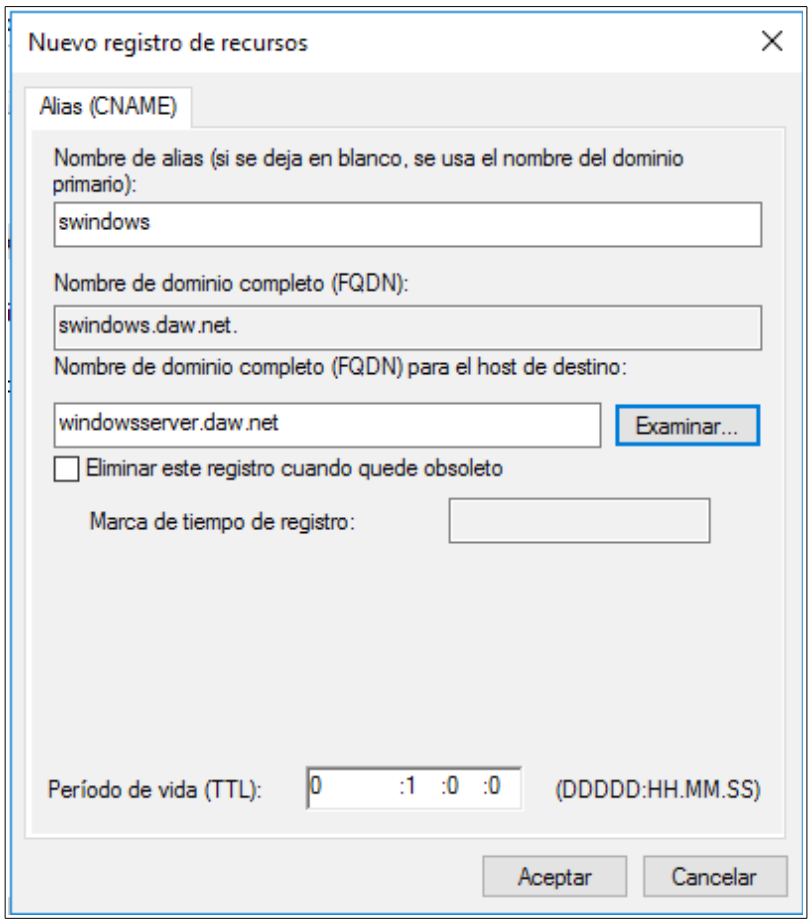
13. Click with the right button on *daw.net* and click on ***NEW ALIASES (CNAME)***

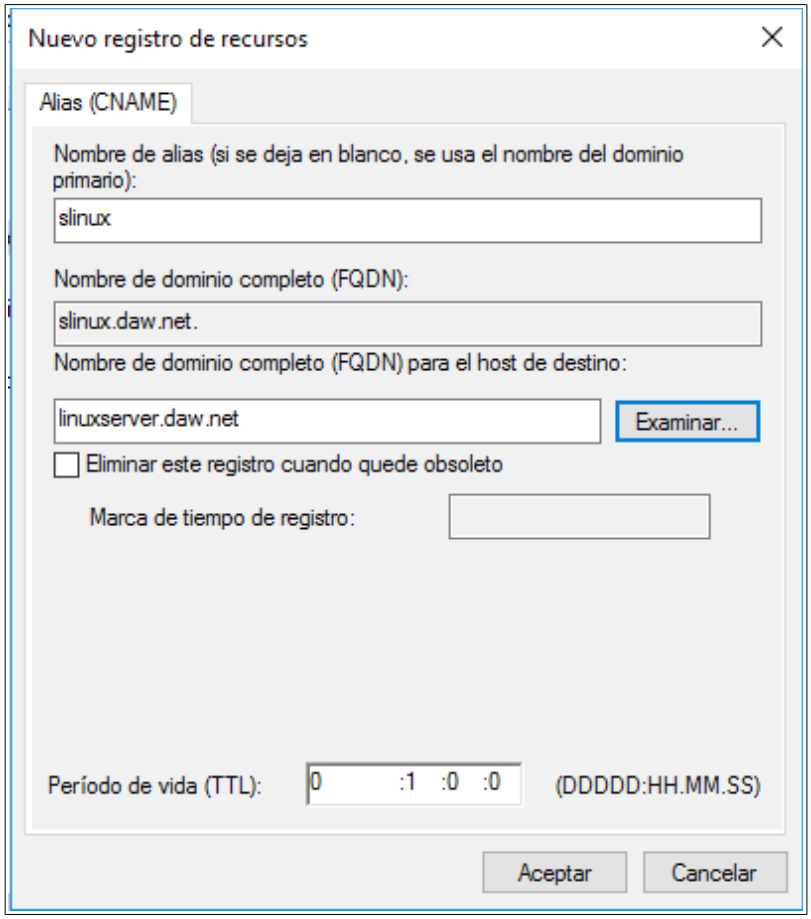



14. Write the alias and the name. Click on ***BROWSE*** to select the ***A*** records created

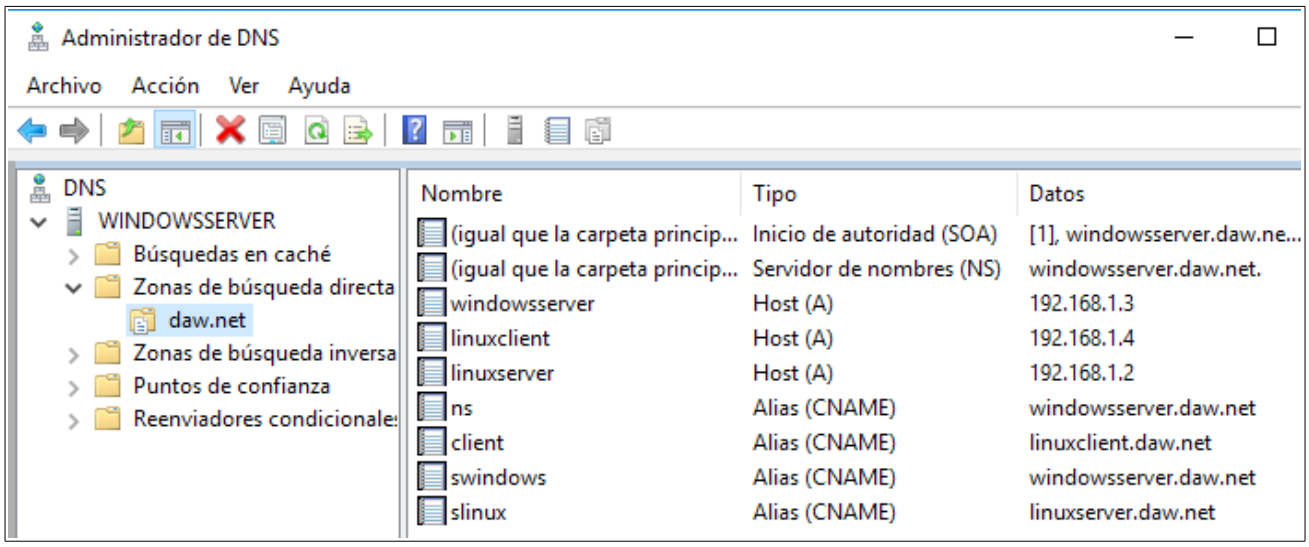

Nuevo registro de recursos
Alias (CNAME)
Nombre de alias (si se deja en blanco, se usa el nombre del dominio primario):
ns
Nombre de dominio completo (FQDN):
ns.daw.net.
Nombre de dominio completo (FQDN) para el host de destino:
windowsserver.daw.net
Examinar...
Eliminar este registro cuando quede obsoleto
Marca de tiempo de registro:
Período de vida (TTL):
0 :1 :0 :0
(DDDDD:HH.MM.SS)
Aceptar
Cancelar
Examinar
Buscar en:
daw.net
Registros:
Nombre
Tipo
Datos
Marca de t...
windowsse...
Host (A)
192.168.1.3
static
linuxclient
Host (A)
192.168.1.4
linuxserver
Host (A)
192.168.1.2
Selección:
windowsserver.daw.net
Tipos de registro:
Hosts y alias (registros A y CNAME)
Aceptar
Cancelar


Nuevo registro de recursos
Alias (CNAME)
Nombre de alias (si se deja en blanco, se usa el nombre del dominio primario):
client
Nombre de dominio completo (FQDN):
client.daw.net.
Nombre de dominio completo (FQDN) para el host de destino:
linuxclient.daw.net
Examinar...
Eliminar este registro cuando quede obsoleto
Marca de tiempo de registro:
Período de vida (TTL):
0 :1 :0 :0
(DDDDD:HH.MM.SS)
Aceptar
Cancelar


Nuevo registro de recursos
Alias (CNAME)
Nombre de alias (si se deja en blanco, se usa el nombre del dominio primario):
swindows
Nombre de dominio completo (FQDN):
swindows.daw.net.
Nombre de dominio completo (FQDN) para el host de destino:
windowsserver.daw.net
Examinar...
Eliminar este registro cuando quede obsoleto
Marca de tiempo de registro:
Período de vida (TTL):
0 :1 :0 :0
(DDDDD:HH.MM.SS)
Aceptar
Cancelar




15. You can see all the configuration.



Now we can check the configuration using ***nslookup***

```
C:\Windows\system32>nslookup linuxclient.daw.net
Servidor:  localhost
Address:  127.0.0.1

Nombre:  linuxclient.daw.net
Address:  192.168.1.4


C:\Windows\system32>nslookup client
Servidor:  localhost
Address:  127.0.0.1

Nombre:  linuxclient.daw.net
Address:  192.168.1.4
Aliases:  client.daw.net
```

## 2.3 Configuring DNS server in WS2016 (primary, reverse lookup zone)

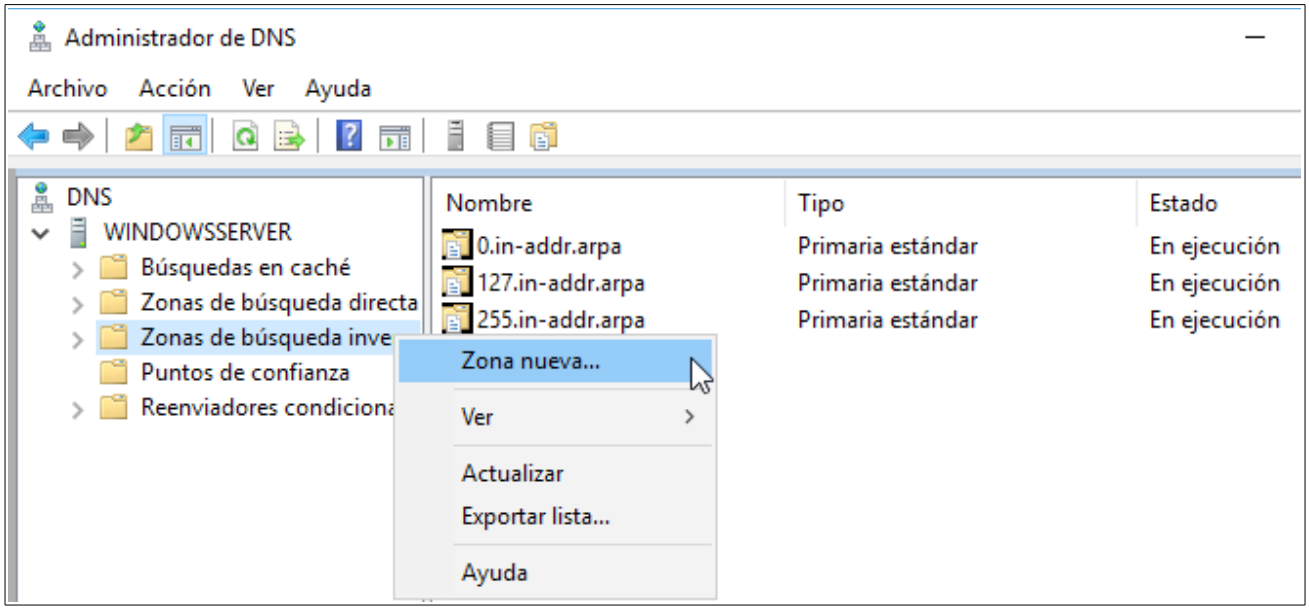
Now we are going to configure the DNS server as primary to a **reverse lookup zone**, so in this case:

- The server will only works to the local network (not to hosts from Internet).
- The server will works as master (primary) and it will have authority to the reverse lookup zone for the network 192.168.1.0:
  - Dynamic updates will not allowed.
  - The primary DNS server will be *serverwindows.daw.net* (**NS record**).
  - We will use the IP addresses explained above (**PTR record**).

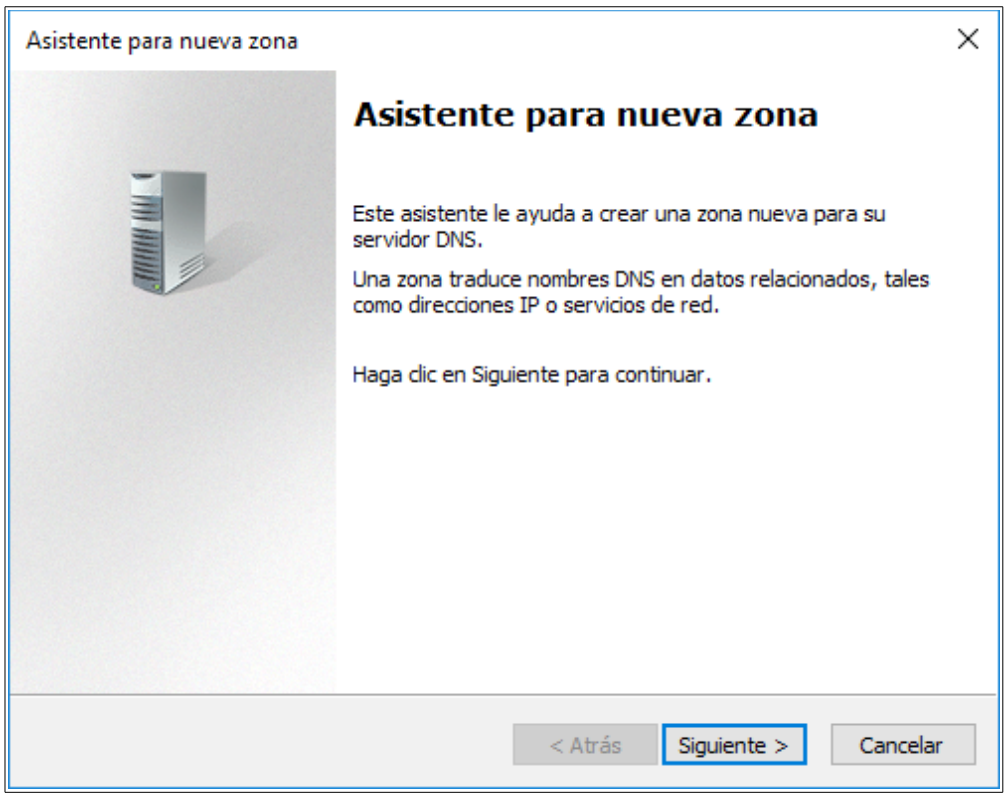
### 2.3.1 Configuring the reverse lookup zone

To configure the reverse lookup zone we will follow these steps:

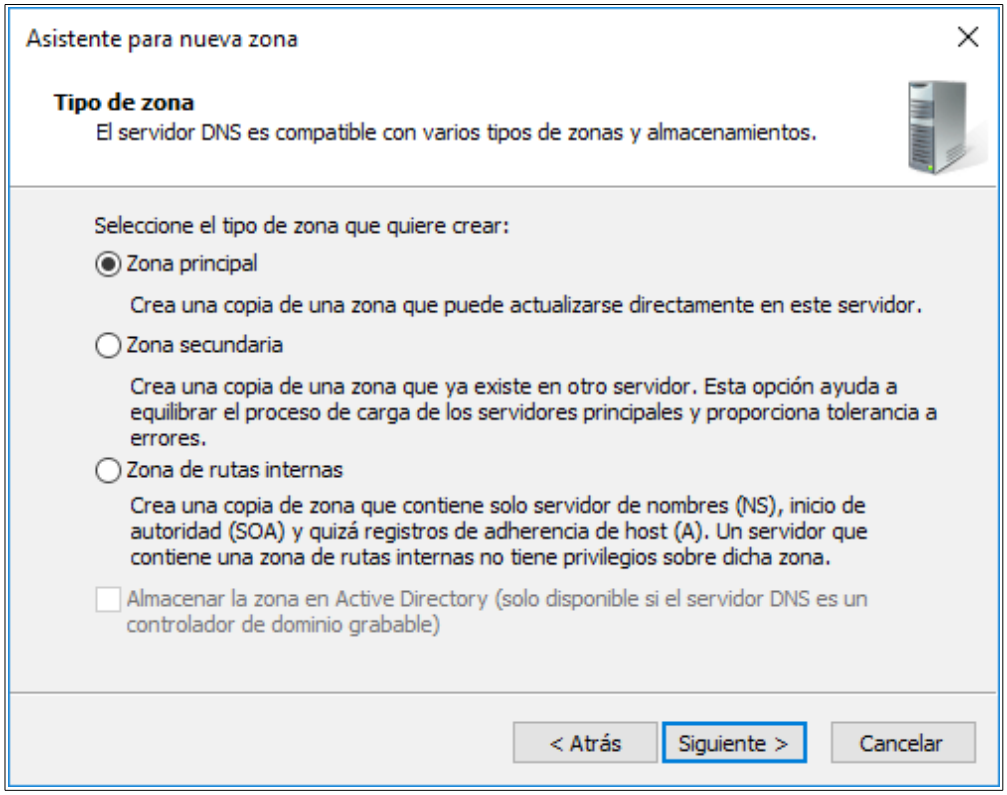
1. Go to the server administration window, click with the right button on ***REVERSE LOOKUP ZONE*** and click on ***NEW ZONE***



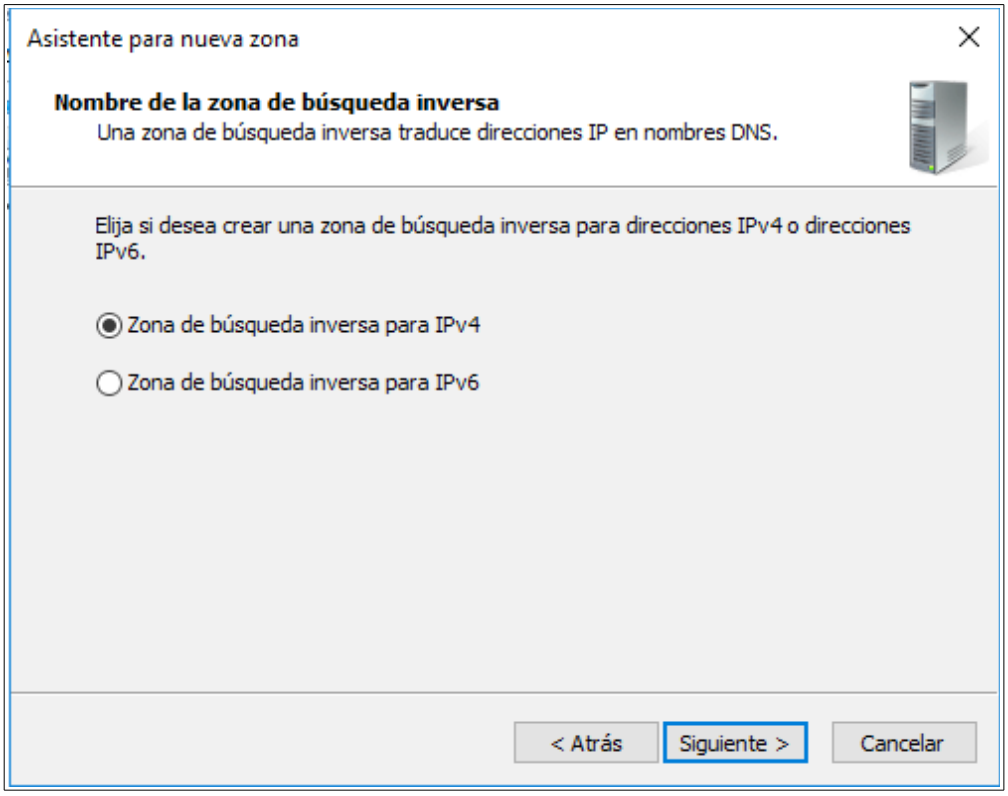

2. Read the information of the wizard and click on ***NEXT***



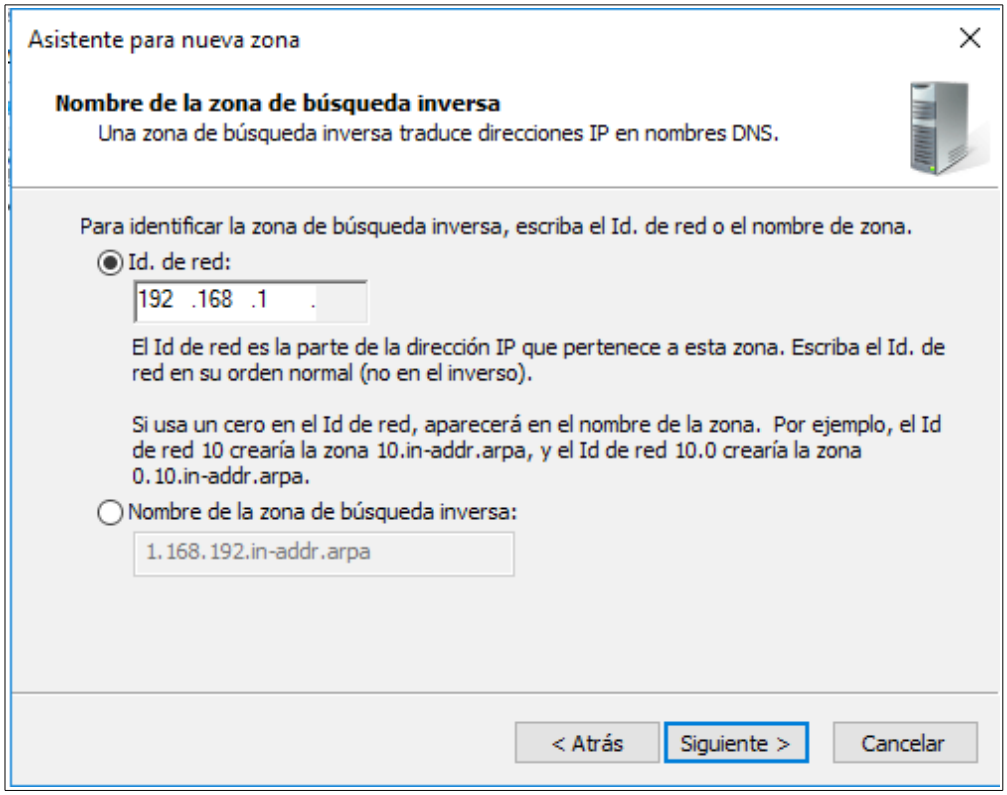
3. Select ***PRIMARY ZONE*** and click on ***NEXT***



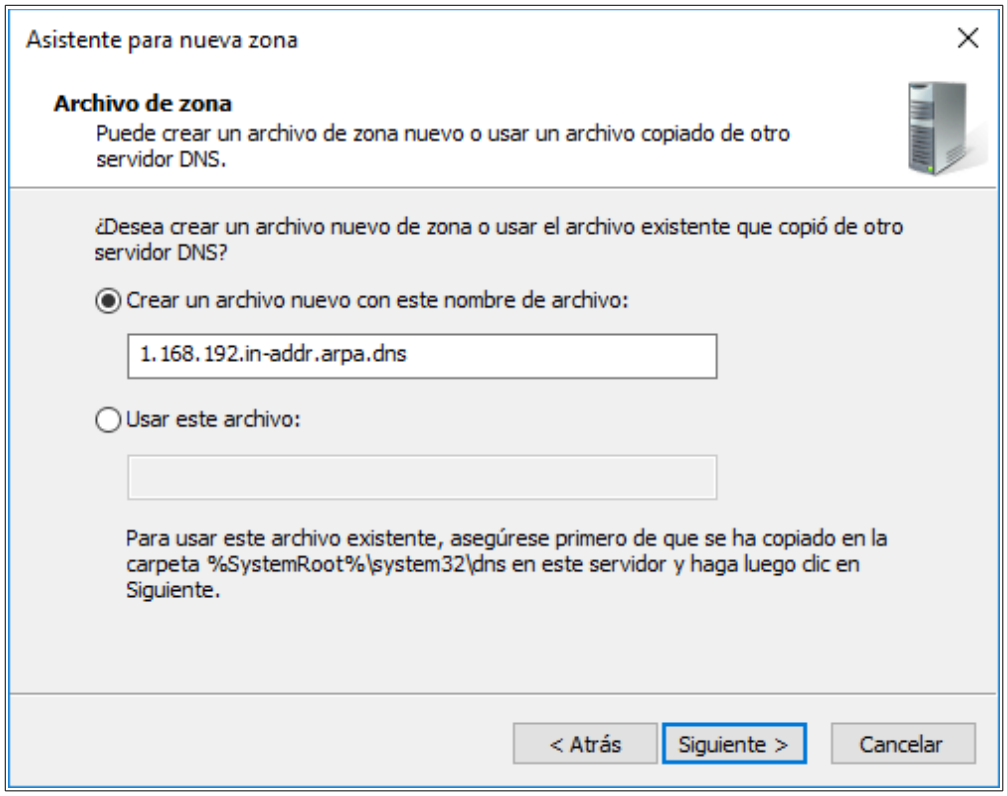

4. Select ***IPV4 REVERSE LOOKUP ZONE*** and click on ***NEXT***



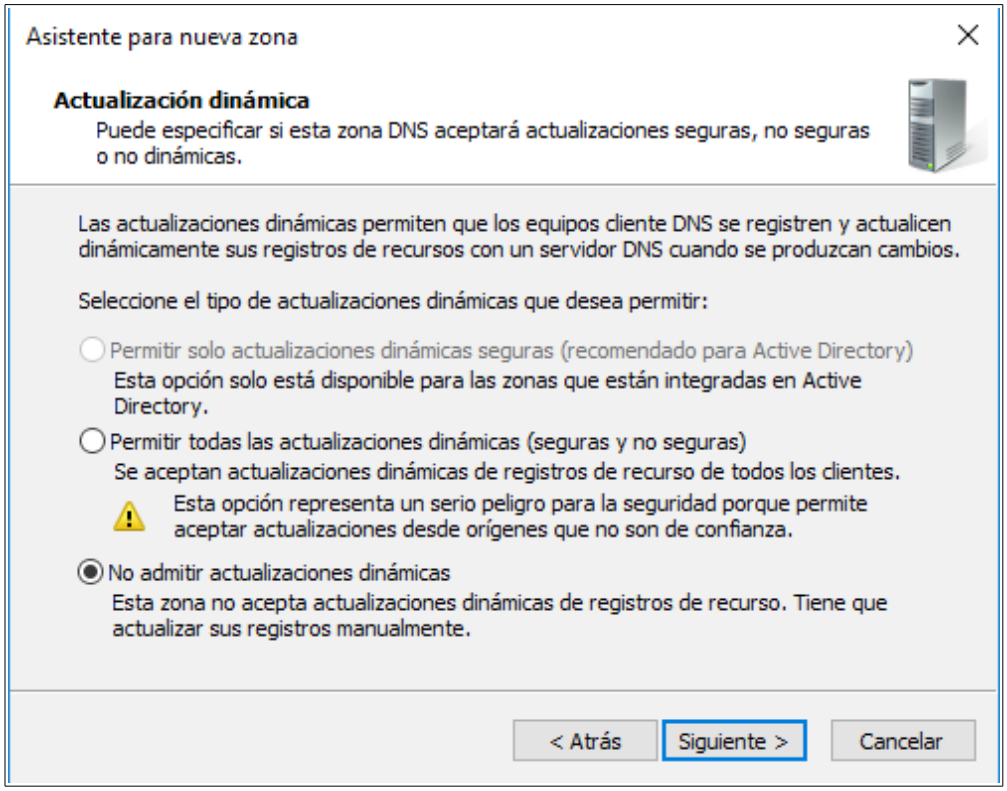

5. Write 192.168.1 as network identification (you can see the name) and click on ***NEXT***



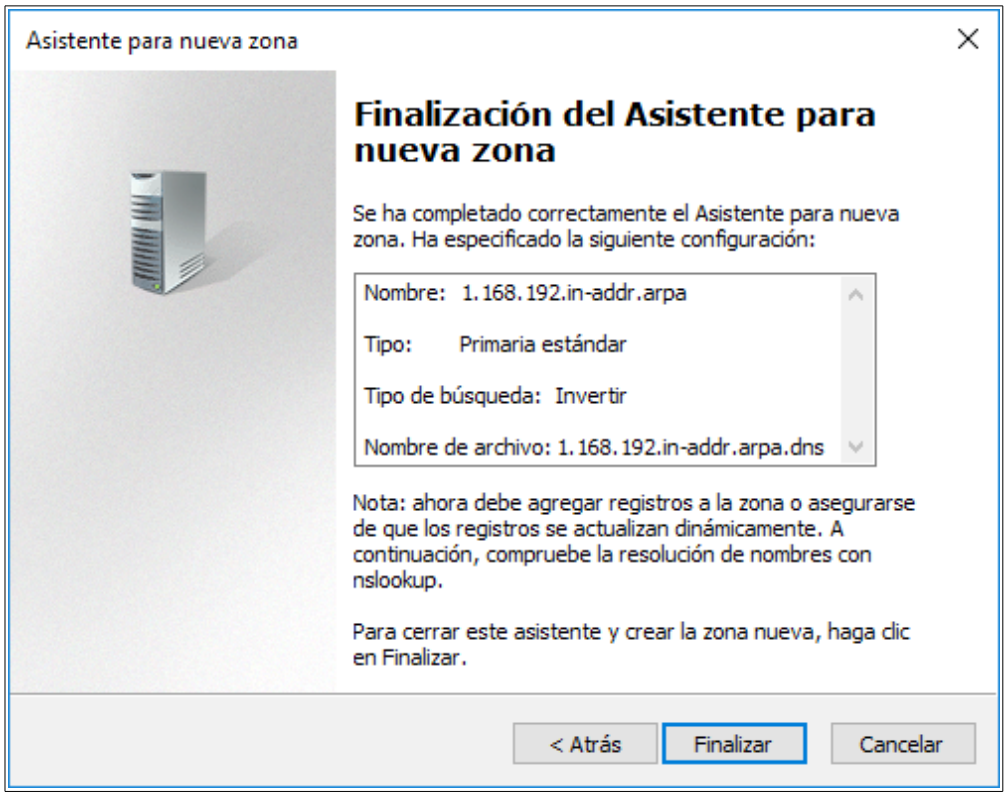
6. Select the option C***REATE A NEW FILE WITH THIS FILE NAME***



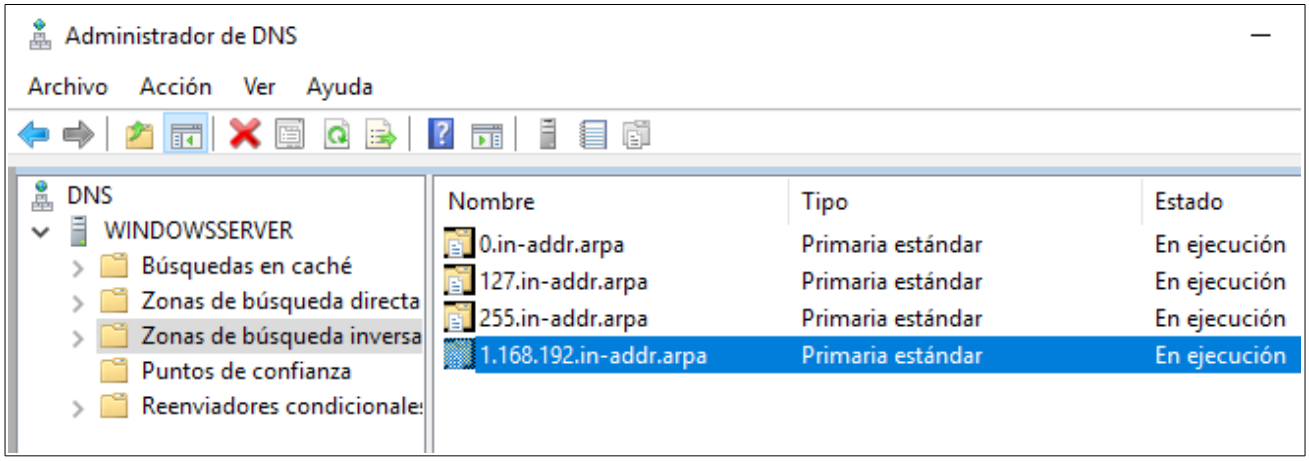

7. Select the option of ***DO NOT ALLOW DYNAMIC UPDATES*** and click on ***NEXT***



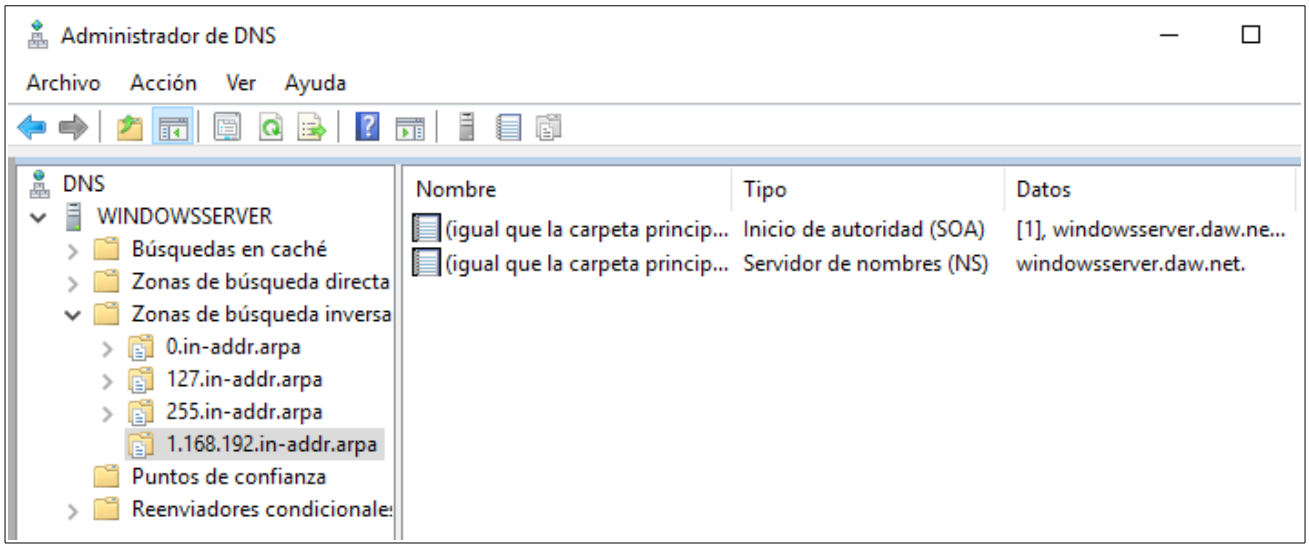

8. Read the summary and click on ***FINISH***



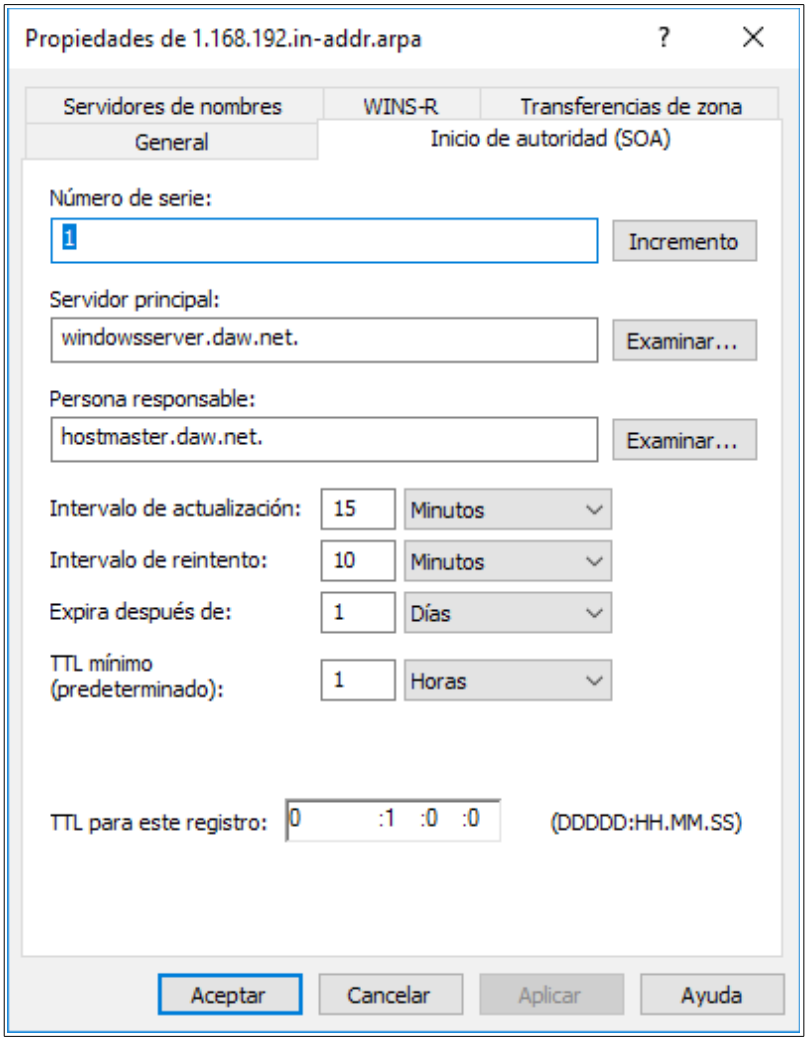
You can see that there is a new entry in ***REVERSE LOOKUP ZONES***



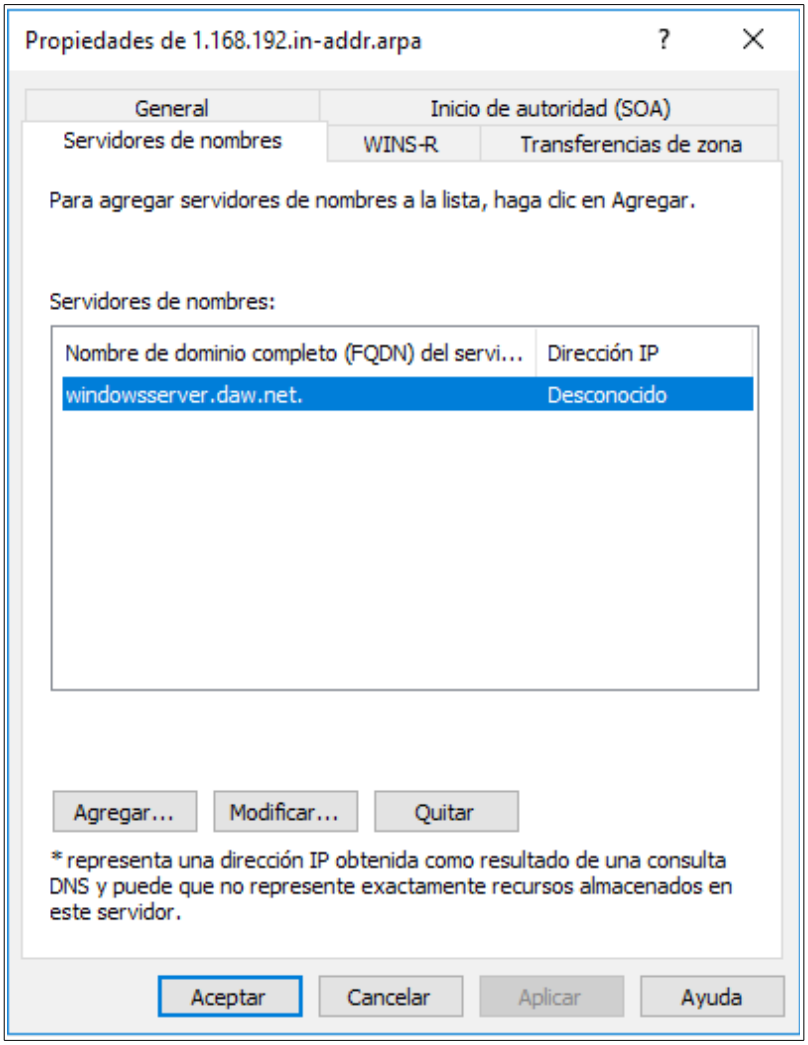

9. Click twice on ***1.168.192.in-addr.arpa*** and you will see the ***SOA*** and ***NS*** records.




10. Click twice on the ***SOA*** record and see its properties.

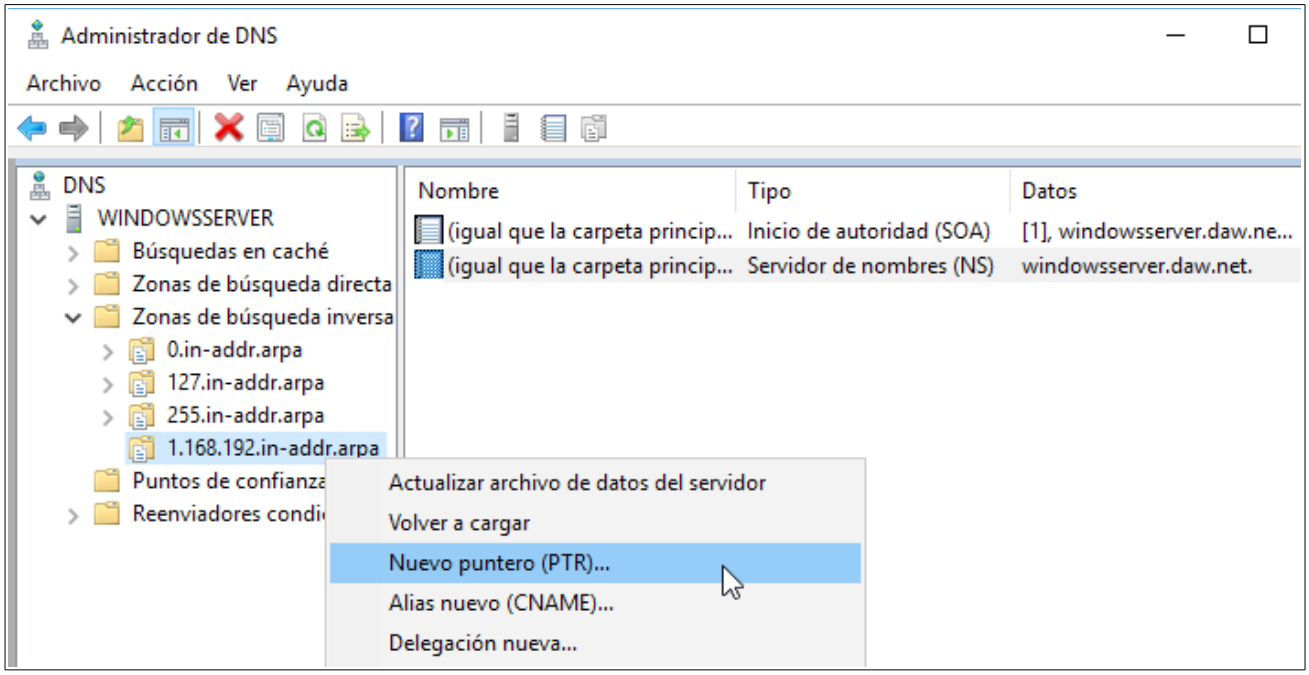



11. Click twice on the ***NS*** record and see its properties. You can see that the IP address is known because there is a ***A*** record created, in the section before, for the name *windowsserver.daw.net*



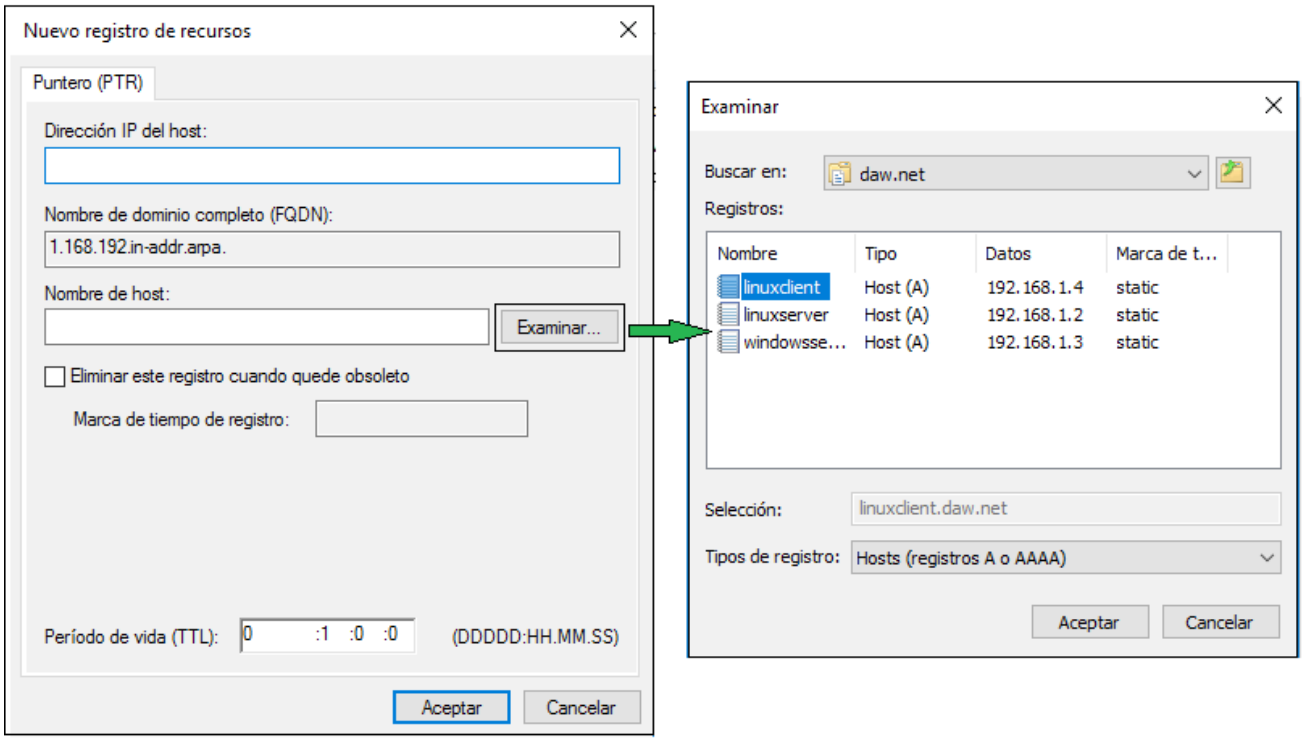

Now we are to create the **PTR** records for the names of the virtual machines

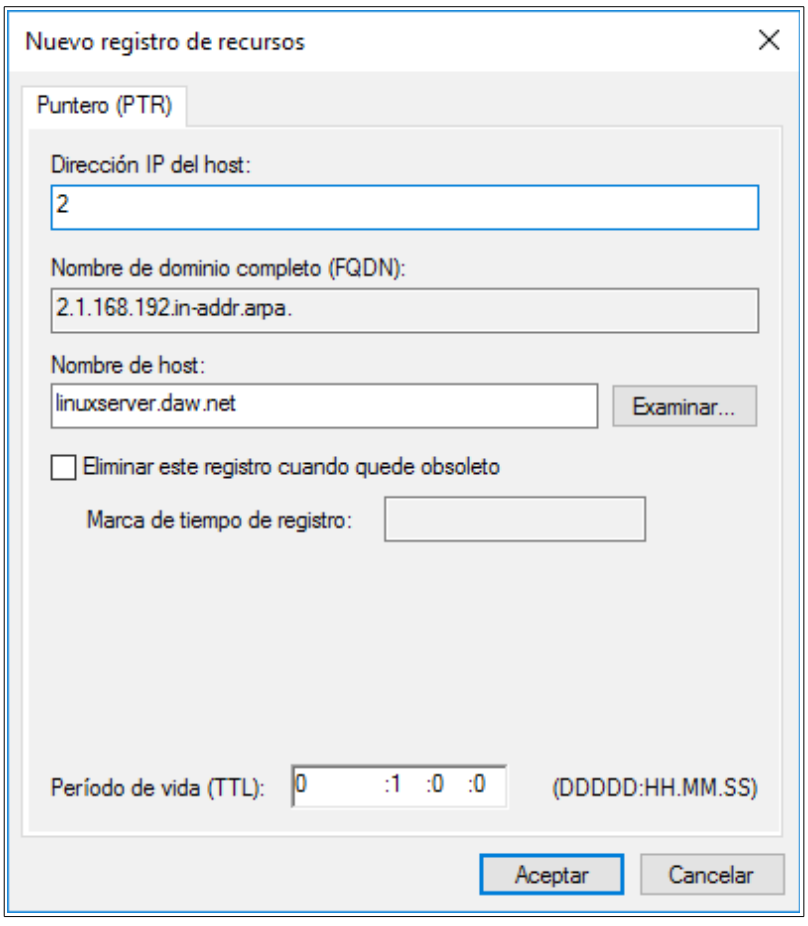
12. Click with the right button on the zone ***1.68.192.in-addr.arpa*** and select ***NEW POINTER (PTR)***

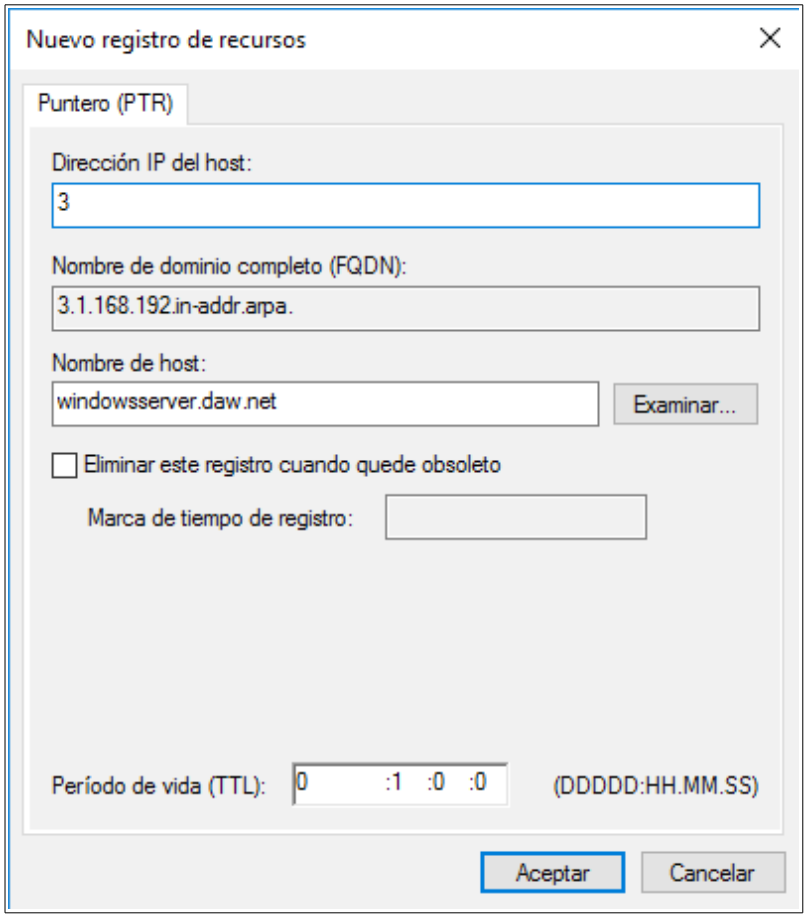


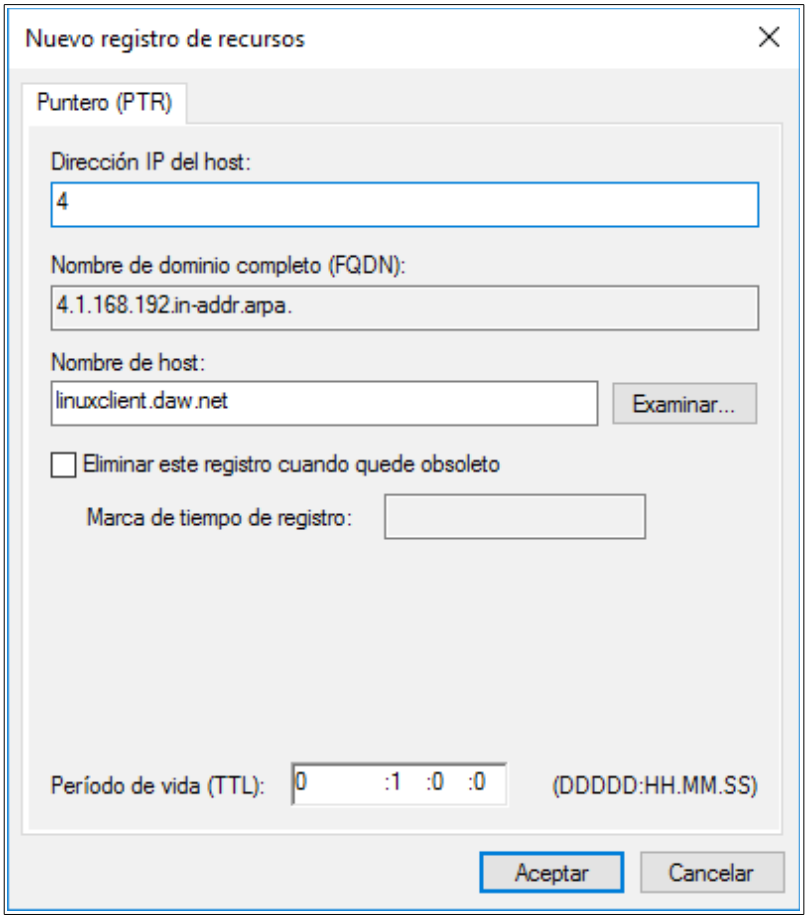

13. Write the host part of the IP address and the name associated. We can click on ***BROWSE*** and select the ***A*** records created before.

> Our network IP address is **192.168.1.0** and the netmask is **255.255.255.0**. This means that the first three bytes (numbers in the IP address) identify the network and only the last byte identify the host. For this reason, when we are configuring the host *linuxserver.daw.net* (192.168.1.**2**) we write a **2** in the IP address of the host.

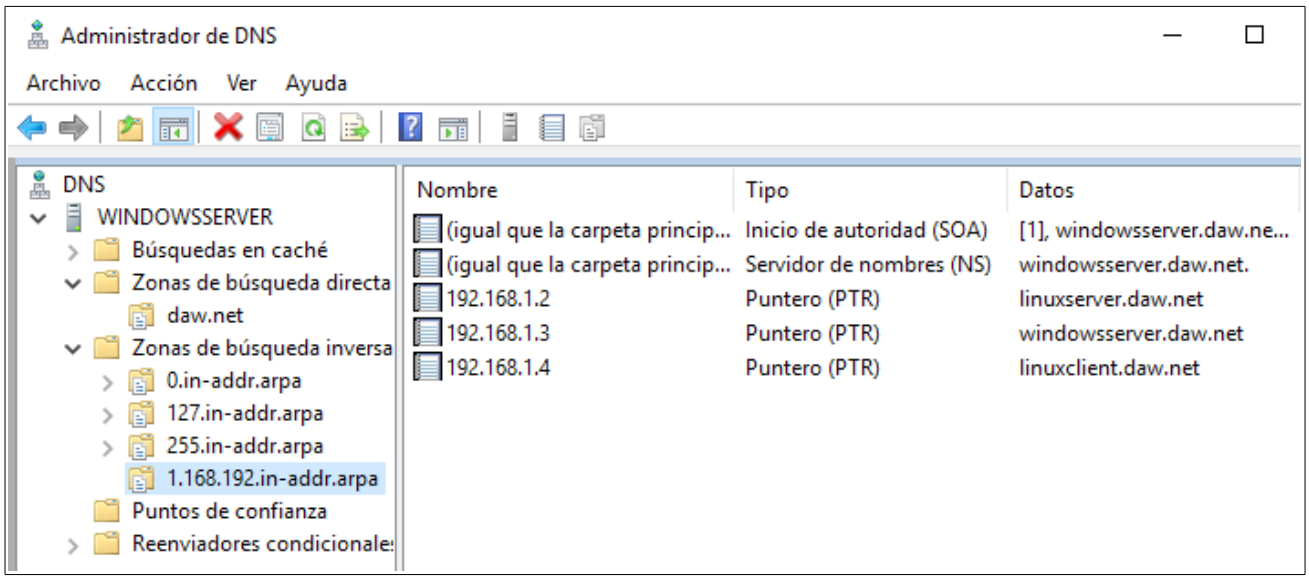

Nuevo registro de recursos
Puntero (PTR)
Dirección IP del host:
Nombre de dominio completo (FQDN):
1.168.192.in-addr.arpa.
Nombre de host:
Examinar...
Eliminar este registro cuando quede obsoleto
Marca de tiempo de registro:
Período de vida (TTL):
0 :1 :0 :0
(DDDDD:HH.MM.SS)
Aceptar
Cancelar
Examinar
Buscar en:
daw.net
Registros:
Nombre
Tipo
Datos
Marca de t...
linuxclient
Host (A)
192.168.1.4
static
linuxserver
Host (A)
192.168.1.2
static
windowsse...
Host (A)
192.168.1.3
static
Selección:
linuxclient.daw.net
Tipos de registro:
Hosts (registros A o AAAA)
Aceptar
Cancelar


Nuevo registro de recursos
Puntero (PTR)
Dirección IP del host:
2
Nombre de dominio completo (FQDN):
2.1.168.192.in-addr.arpa.
Nombre de host:
linuxserver.daw.net
Examinar...
Eliminar este registro cuando quede obsoleto
Marca de tiempo de registro:
Período de vida (TTL):
0 :1 :0 :0
(DDDDD:HH.MM.SS)
Aceptar
Cancelar


Nuevo registro de recursos
Puntero (PTR)
Dirección IP del host:
3
Nombre de dominio completo (FQDN):
3.1.168.192.in-addr.arpa.
Nombre de host:
windowsserver.daw.net
Examinar...
Eliminar este registro cuando quede obsoleto
Marca de tiempo de registro:
Período de vida (TTL):
0 :1 :0 :0
(DDDDD:HH.MM.SS)
Aceptar
Cancelar




14. You can see all the configuration.



Now we can check the configuration using **nslookup**

```
C:\Windows\system32>nslookup 192.168.1.4
Servidor:  localhost
Address:  127.0.0.1

Nombre:  linuxclient.daw.net
Address:  192.168.1.4
```

## 2.4 Configuring DNS server in Linux

### 2.4.1 Installing the server

In Linux we will use the software **bind**, which is an open source software that implements the DNS.

To install it we have to write in a terminal: ***sudo apt-get install bind9***

If the installation fails we will update the ubuntu repositories: ***sudo apt-get update***

and then ***sudo apt-get install bind9*** again.

Once installed we can see its directory in /etc/bind

```
administrador@LinuxServer:/etc/bind$ ls
bind.keys   db.empty    named.conf.default-zones  zones.rfc1918
db.0        db.local    named.conf.local
db.127      db.root     named.conf.options
db.255      named.conf  rndc.key
```

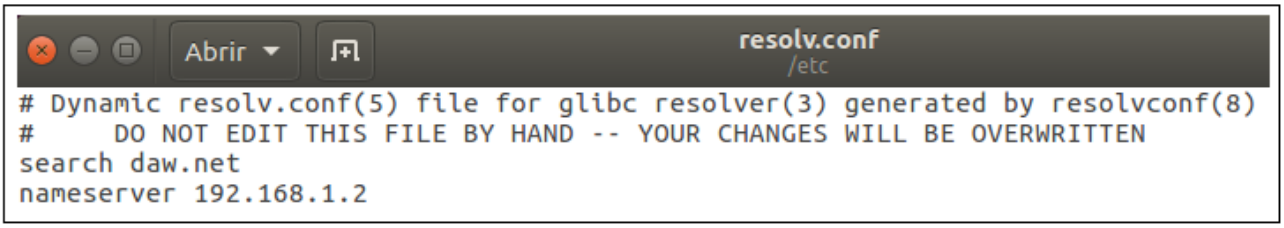
We can take a look to some files:

```
administrador@LinuxServer:/etc/bind$ cat named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

```
administrador@LinuxServer:/etc/bind$ cat named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

### 2.4.2 Configuring the forward and reverse lookup zone

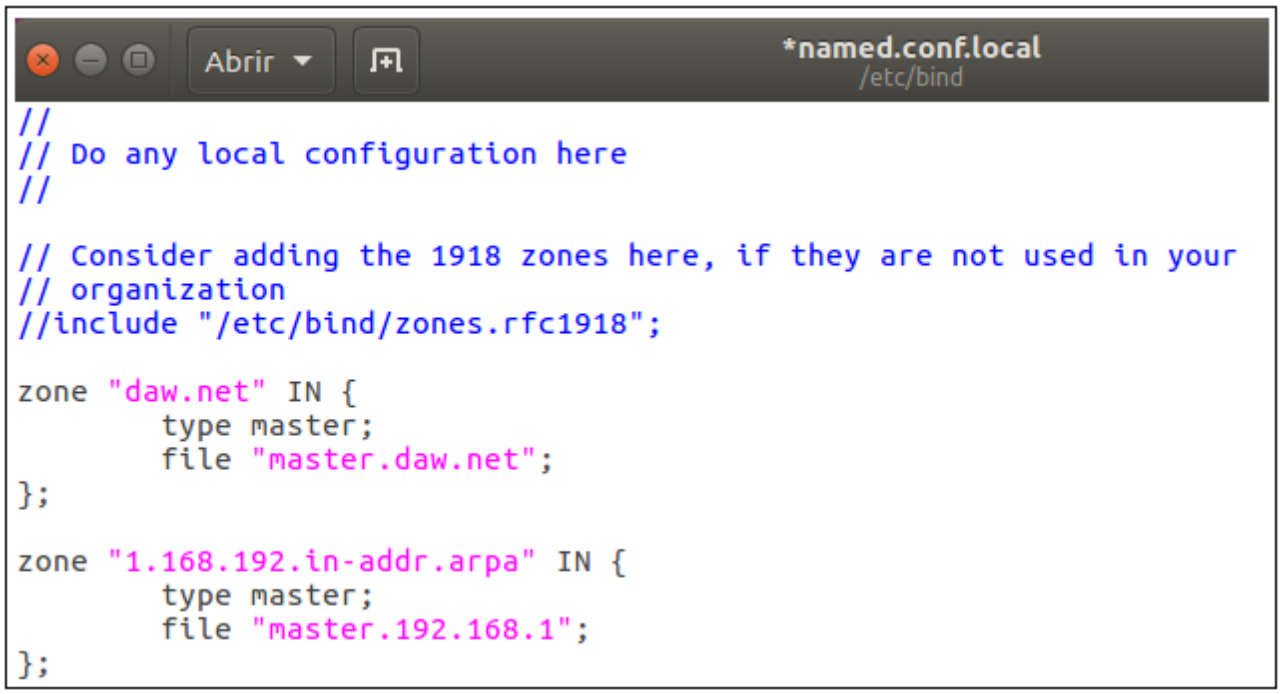
First it is important to insert the IP address of the server (192.168.1.2) and the domain (*daw.net*) in the */etc/resolv.conf* file:



Now we are to configure both lookup zones at the same time: forward and reverse. For it, we have to follow these steps:

1. Open the *named.conf.local* and create the two zones:
    1. Forward:
        1. name: *daw.net*
        2. type: master (primary)
        3. configuration file: *master.daw.net* (we will create this file).
    2. Reverse:
        1. name: *1.168.192.in-addr.arpa*
        2. type: master (primary)
        3. configuration file: *master.192.168.1* (we will create this file).

Write ***sudo gedit /etc/named.conf.local*** in the terminal and modify the file:




2. Now, we are going to copy the default files and create our master files:

***sudo cp db.local master.daw.net***

***sudo cp db.127 master.192.168.1***

3. Modify the *master.daw.net* file and include the **NS** and **A** records (one record for each machine). IMPORTANT '.'

> In these files the final **.** (dot) in the domain is very important because identify the **root domain**.

*master.daw.net
/etc/bind

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     linuxserver.daw.net. root.linuxserver.daw.net. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@               IN      NS      linuxserver.daw.net.
@               IN      A       192.168.1.2
linuxserver     IN      A               192.168.1.2
windowsserver   IN      A               192.168.1.3
windowsclient   IN      A               192.168.1.4
```

4. Now, modify the *master.192.168.1* file and include the **NS** and **PTR** records (one for each machine).

master.192.168.1
/etc/bind

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     linuxserver.daw.net. root.linuxserver.daw.net. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      linuxserver.daw.net.
2       IN      PTR     linuxserver.daw.net.
3       IN      PTR     windowsserver.daw.net.
4       IN      PTR     windowsclient.daw.net.
```

5. To check errors in the named files we write: ***named-checkconf***. If there are not any error everything will be right.

```
administrador@LinuxServer:/etc/bind$ named-checkconf
administrador@LinuxServer:/etc/bind$
```

6. Now we copy the master files to the **cache**

```
administrador@LinuxServer:/etc/bind$ sudo cp /etc/bind/master.daw.net /var/cache
/bind
administrador@LinuxServer:/etc/bind$ sudo cp /etc/bind/master.192.168.1 /var/cac
he/bind
```

7. Start or restart the service: ***sudo /etc/init.d/bind9 restart***

```
administrador@LinuxServer:/etc/bind$ sudo /etc/init.d/bind9 restart
[ ok ] Restarting bind9 (via systemctl): bind9.service.
```

8. We can see the status of the server: ***sudo /etc/init.d/bind9 status***

```
administrador@LinuxServer:/etc/bind$ sudo /etc/init.d/bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
  Drop-In: /run/systemd/generator/bind9.service.d
           └─50-insserv.conf-$named.conf
   Active: active (running) since jue 2016-09-29 18:18:51 CEST; 5s ago
     Docs: man:named(8)
  Process: 4103 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 4108 (named)
    Tasks: 4 (limit: 512)
   CGroup: /system.slice/bind9.service
           └─4108 /usr/sbin/named -f -u bind

sep 29 18:18:52 LinuxServer named[4108]: managed-keys-zone: loaded serial 3
sep 29 18:18:52 LinuxServer named[4108]: zone 0.in-addr.arpa/IN: loaded serial 1
sep 29 18:18:52 LinuxServer named[4108]: zone 1.168.192.in-addr.arpa/IN: loaded serial 1
sep 29 18:18:52 LinuxServer named[4108]: zone daw.net/IN: loaded serial 2
sep 29 18:18:52 LinuxServer named[4108]: zone 255.in-addr.arpa/IN: loaded serial 1
sep 29 18:18:52 LinuxServer named[4108]: zone 127.in-addr.arpa/IN: loaded serial 1
sep 29 18:18:52 LinuxServer named[4108]: zone localhost/IN: loaded serial 2
sep 29 18:18:52 LinuxServer named[4108]: all zones loaded
sep 29 18:18:52 LinuxServer named[4108]: running
```

Now we can check the configuration using ***dig*** for the forward lookup and ***nslookup*** for the reverse.

```
administrador@LinuxServer:/etc/bind$ dig linuxserver.daw.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> linuxserver.daw.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39512
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;linuxserver.daw.net.           IN      A

;; ANSWER SECTION:
linuxserver.daw.net.    604800  IN      A       192.168.1.2

;; AUTHORITY SECTION:
daw.net.                604800  IN      NS      linuxserver.daw.net.

;; Query time: 0 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Thu Sep 29 18:13:01 CEST 2016
;; MSG SIZE  rcvd: 78
```

```
administrador@LinuxServer:/etc/bind$ dig windowsclient.daw.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> windowsclient.daw.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63007
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;windowsclient.daw.net.         IN      A

;; ANSWER SECTION:
windowsclient.daw.net.  604800  IN      A       192.168.1.4

;; AUTHORITY SECTION:
daw.net.                604800  IN      NS      linuxserver.daw.net.

;; ADDITIONAL SECTION:
linuxserver.daw.net.    604800  IN      A       192.168.1.2

;; Query time: 0 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Thu Sep 29 18:13:48 CEST 2016
;; MSG SIZE  rcvd: 108
```

```
administrador@LinuxServer:/etc/bind$ nslookup 192.168.1.3
Server:         192.168.1.2
Address:        192.168.1.2#53

3.1.168.192.in-addr.arpa        name = windowsserver.daw.net.
```

## 2.5 Configuring the client

Now we to configure the client and change the dns server used in the network interface. For that, we have to modify the file /etc/network/interfaces and set the dns-nameservers to 192.168.1.2 or 192.168.1.3

```
administrador@LinuxClient:~$ sudo gedit /etc/network/interfaces
```

Abrir — interfaces /etc/network

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
auto enp0s3
iface enp0s3 inet static
address 192.168.1.4
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 192.168.1.3
```

And then we have to restart the web service to apply the changes: ***sudo service networking restart***

```
administrador@LinuxClient:~$ dig linuxserver.daw.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> linuxserver.daw.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52889
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;linuxserver.daw.net.           IN      A

;; ANSWER SECTION:
linuxserver.daw.net.    3600    IN      A       192.168.1.2

;; Query time: 0 msec
;; SERVER: 192.168.1.3#53(192.168.1.3)
;; WHEN: Mon Sep 18 10:48:24 CEST 2017
;; MSG SIZE  rcvd: 64
```

## 3. FTP

In this section we are going to install and configure the FTP server in Linux.

### 3.1 Installing FTP server

To install the FTP sever we use the **vsftpd** packet. For that we have to write in the terminal:
sudo apt-get install vsftpd

If the installation fails we will update the Ubuntu repositories: **sudo apt-get update**
and then **sudo apt-get install vsftpd** again.

It will create the following:

- The configuration files.
- The user and group *ftp*.
- The directory */srv/ftp*.
  - Its owner is *root* and its group is *ftp*.

```
administrador@LinuxServer:/srv$ ls -l
total 4
drwxr-xr-x 2 root ftp 4096 oct 29 17:28 ftp
```

- It is the default directory of the anonymous users (they do not need to identify them to access).

Once installed, we can check if the server is running and listening in port 21/TCP. We have to write **ps -ef | grep vsftpd** and then **netstat -ltn**

```
administrador@LinuxServer:~$ ps -ef | grep vsftpd
root      2477     1  0 17:28 ?        00:00:00 /usr/sbin/vsftpd /etc/vsftpd.con
f
adminis+  2541  1883  0 17:29 pts/6    00:00:00 grep --color=auto vsftpd
administrador@LinuxServer:~$ netstat -ltn
Conexiones activas de Internet (solo servidores)
Proto  Recib Enviad Dirección local          Dirección remota        Estado
tcp         0      0 192.168.1.2:53          0.0.0.0:*               ESCUCHAR
tcp         0      0 127.0.0.1:53            0.0.0.0:*               ESCUCHAR
tcp         0      0 127.0.0.1:631           0.0.0.0:*               ESCUCHAR
tcp         0      0 127.0.0.1:953           0.0.0.0:*               ESCUCHAR
tcp6        0      0 :::80                   :::*                    ESCUCHAR
tcp6        0      0 :::21                   :::*                    ESCUCHAR
tcp6        0      0 :::53                   :::*                    ESCUCHAR
tcp6        0      0 ::1:631                 :::*                    ESCUCHAR
tcp6        0      0 ::1:953                 :::*                    ESCUCHAR
tcp6        0      0 :::443                  :::*                    ESCUCHAR
```

### 3.2 Configuring FTP server

We can see the configuration file in */etc/vsftpd.conf*: **cat /etc/vsftpd.conf**
and we are going to analyse the next directives:

```
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
```

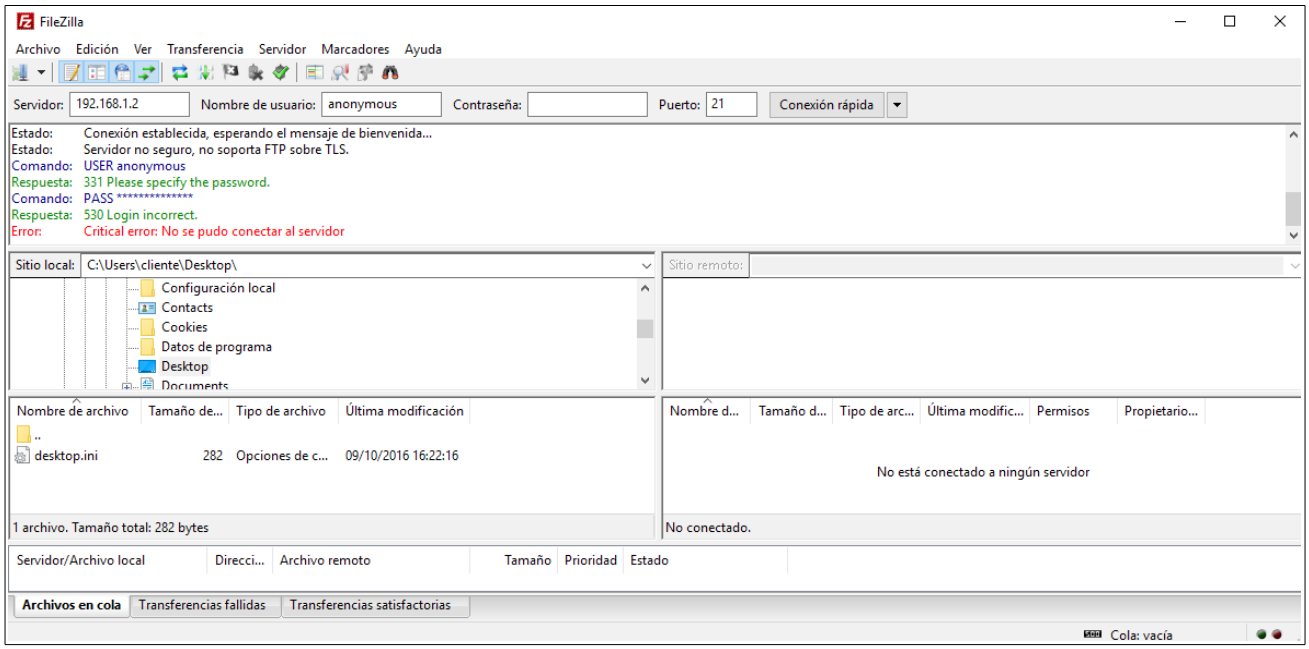
- **anonymous_enable=NO** it is disabled the access to the anonymous users.

- **local_enable=YES** it is enabled the access to the local users.
- **#write_enable=YES** it is commented the directive to allow upload files to the server. So it is forbidden.

Now we are going to test the connection from *linuxclient* or *windowsserver* to *linuxserver*.
For that, we are going to download and install the client Filezilla (it is easy, just follow the wizard leaving everything by default). We can download from:

https://filezilla-project.org/download.php?type=client

Once installed, we are going to try to connect it to *linuxserver* (192.168.1.2) in port 21 being an anonymous user (it does not have password):



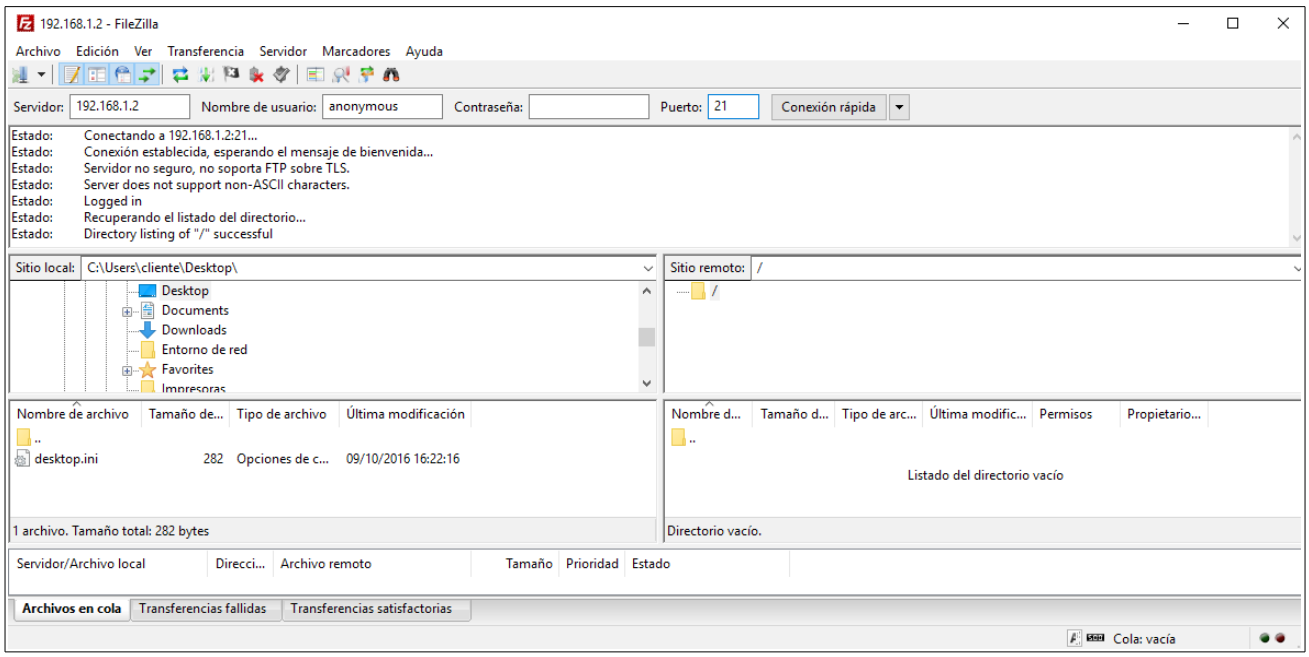

We can see that we can not connect.
Now, we are going to enable the access to anonymous. We are going to edit the configuration file and change **anonymous_enable=NO** to **anonymous_enable=YES**

```
administrador@LinuxServer:~$ sudo gedit /etc/vsftpd.conf
```

vsftpd.conf
/etc

```
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
#
```

Restart the server the server **sudo /etc/init.d/vsftpd restart** and try again:



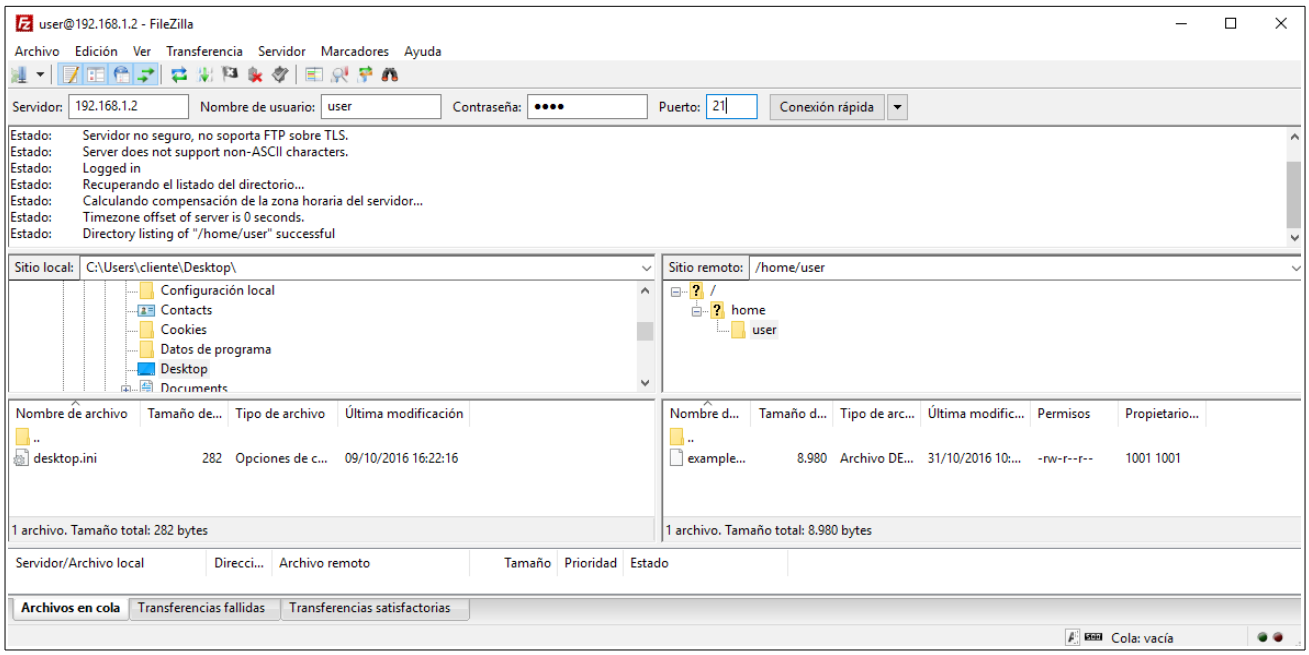

Now we can connect to the server but we can not to transfer files because we are anonymous. So,

we are going to create a new user in *linuxserver* and we are going to try to connect with it.

We create the user *user*

```
administrador@LinuxServer:~$ sudo adduser user
Añadiendo el usuario `user' ...
Añadiendo el nuevo grupo `user' (1001) ...
Añadiendo el nuevo usuario `user' (1001) con grupo `user' ...
Creando el directorio personal `/home/user' ...
Copiando los ficheros desde `/etc/skel' ...
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para user
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []:
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] s
```

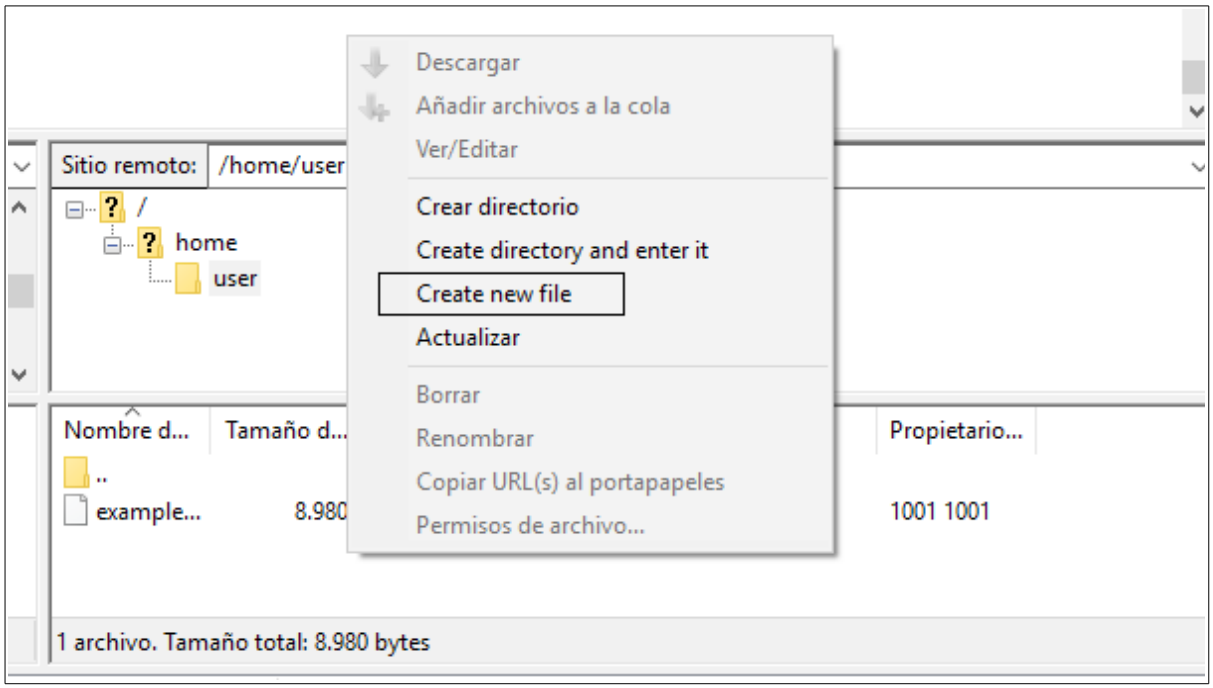
And connect using that user:

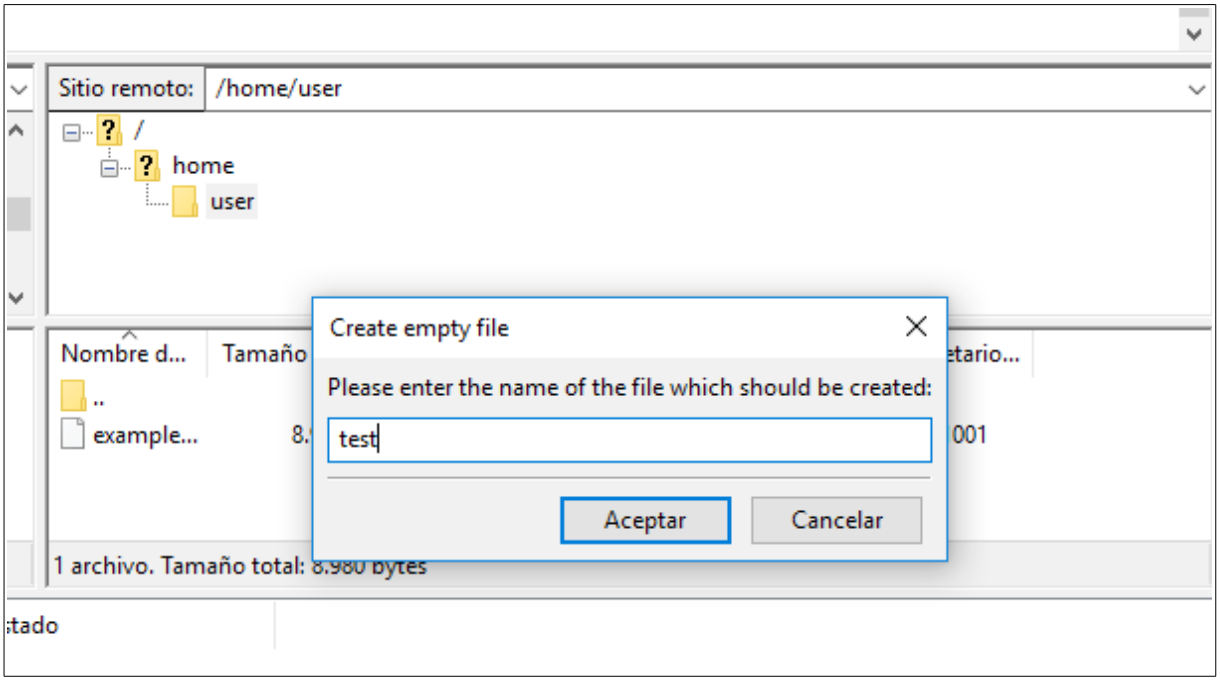


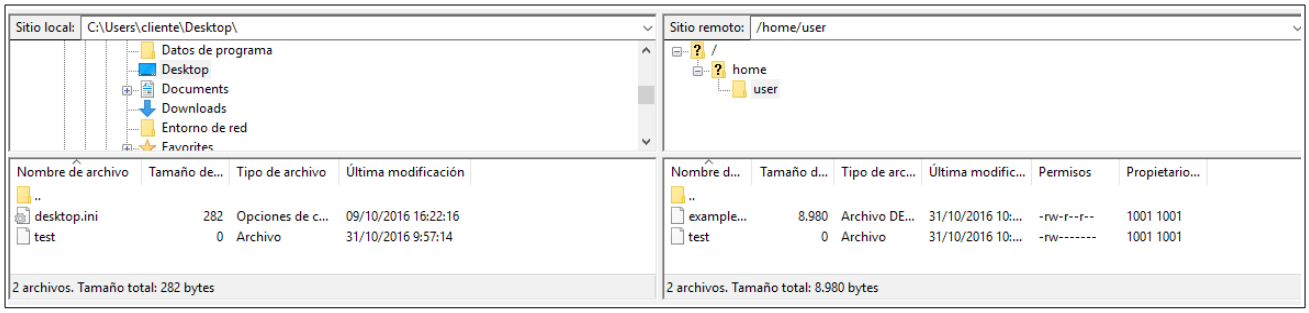

Now we can access but we can not transfer or create any file because of the directive **#write_enable=YES**, so we are going to uncommented it:

```
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

Restart the server, connect again and try to create a file (click with the right button in the right side and click on ***CREATE NEW FILE***) and transfer it (drag it from the right to the left side):






# 4. SSH

## 4.1 Installing SSH server

To install the SSH sever in Linux we use the **openssh** packet. For that we have to write in the terminal:

**sudo apt-get install openssh-server**

If the installation fails we will update the Ubuntu repositories: **sudo apt-get update**

and then **sudo apt-get install openssh-server** again.

It will create the following:

- The configuration files.
- The pair of keys RSA, DSA and ECDSA stored in the directory */etc/ssh*.

Once installed, we can check if the server is running and listening in port 22/TCP. We have to write **ps -ef | grep ssh** and then **netstat -ltn**

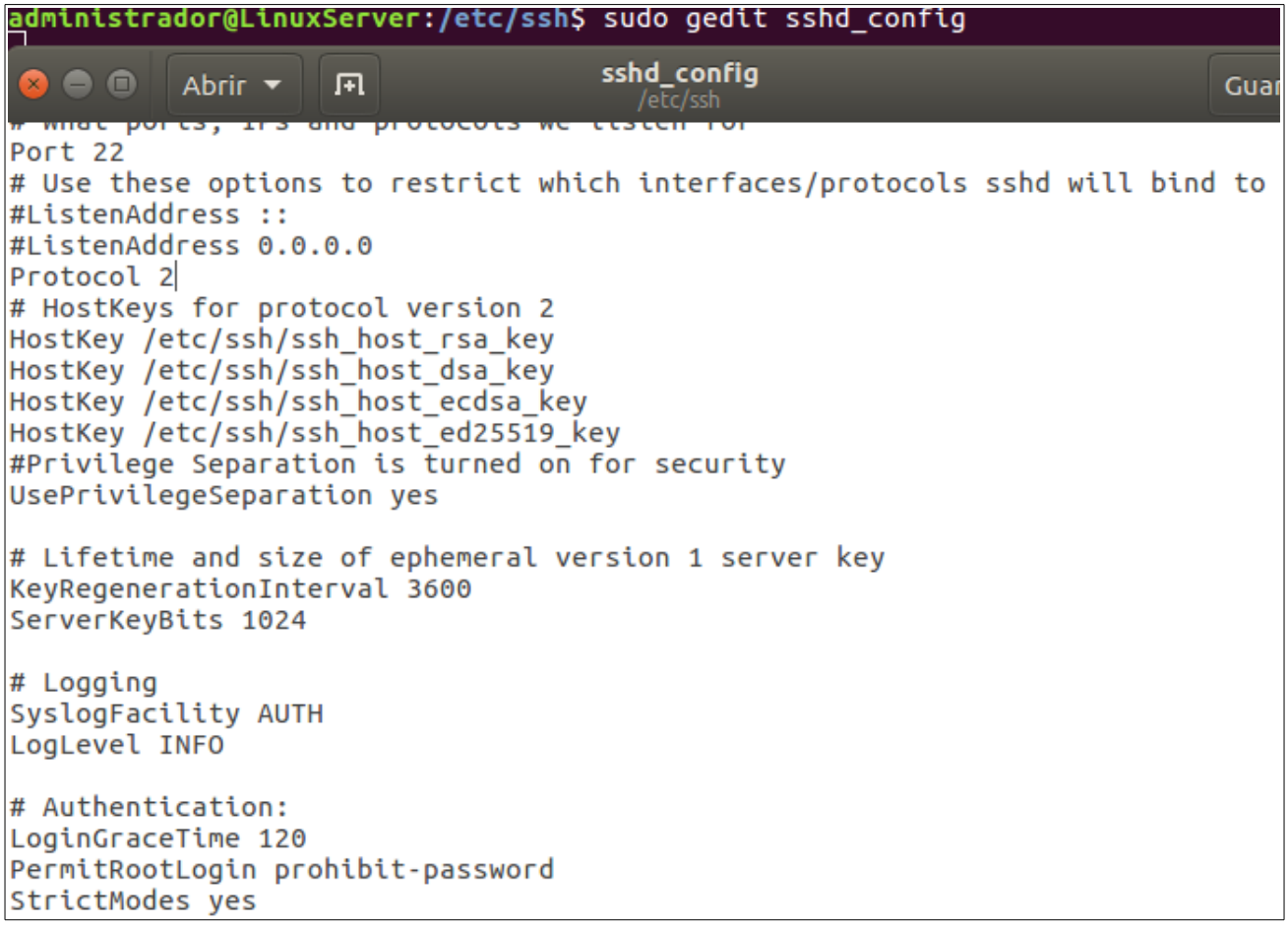
```
administrador@LinuxServer:~$ ps -ef | grep ssh
root     18465     1  0 10:01 ?        00:00:00 /usr/sbin/sshd -D
adminis+ 18540  2326  0 10:03 pts/4    00:00:00 grep --color=auto ssh
administrador@LinuxServer:~$ netstat -ltn
Conexiones activas de Internet (solo servidores)
Proto  Recib Enviad Dirección local          Dirección remota        Estado
tcp        0      0 192.168.1.2:53          0.0.0.0:*               ESCUCHAR
tcp        0      0 127.0.0.1:53            0.0.0.0:*               ESCUCHAR
tcp        0      0 0.0.0.0:22              0.0.0.0:*               ESCUCHAR
tcp        0      0 127.0.0.1:953           0.0.0.0:*               ESCUCHAR
tcp6       0      0 :::80                   :::*                    ESCUCHAR
tcp6       0      0 :::21                   :::*                    ESCUCHAR
tcp6       0      0 :::53                   :::*                    ESCUCHAR
tcp6       0      0 :::22                   :::*                    ESCUCHAR
tcp6       0      0 ::1:953                 :::*                    ESCUCHAR
tcp6       0      0 :::443                  :::*                    ESCUCHAR
```

Also, we can check the public (*.pub) and private keys in the directory */etc/ssh*

```
administrador@LinuxServer:~$ ls -l /etc/ssh
total 340
-rw-r--r-- 1 root root 300261 abr 16  2016 moduli
-rw-r--r-- 1 root root   1756 abr 16  2016 ssh_config
-rw-r--r-- 1 root root   2542 oct 31 10:01 sshd_config
-rw------- 1 root root    672 oct 31 10:01 ssh_host_dsa_key
-rw-r--r-- 1 root root    606 oct 31 10:01 ssh_host_dsa_key.pub
-rw------- 1 root root    227 oct 31 10:01 ssh_host_ecdsa_key
-rw-r--r-- 1 root root    178 oct 31 10:01 ssh_host_ecdsa_key.pub
-rw------- 1 root root    411 oct 31 10:01 ssh_host_ed25519_key
-rw-r--r-- 1 root root     98 oct 31 10:01 ssh_host_ed25519_key.pub
-rw------- 1 root root   1679 oct 31 10:01 ssh_host_rsa_key
-rw-r--r-- 1 root root    398 oct 31 10:01 ssh_host_rsa_key.pub
-rw-r--r-- 1 root root    338 oct 31 10:01 ssh_import_id
```

## 4.2 Configuring SSH server

We can see the configuration file in */etc/ssh/sshd_config*:



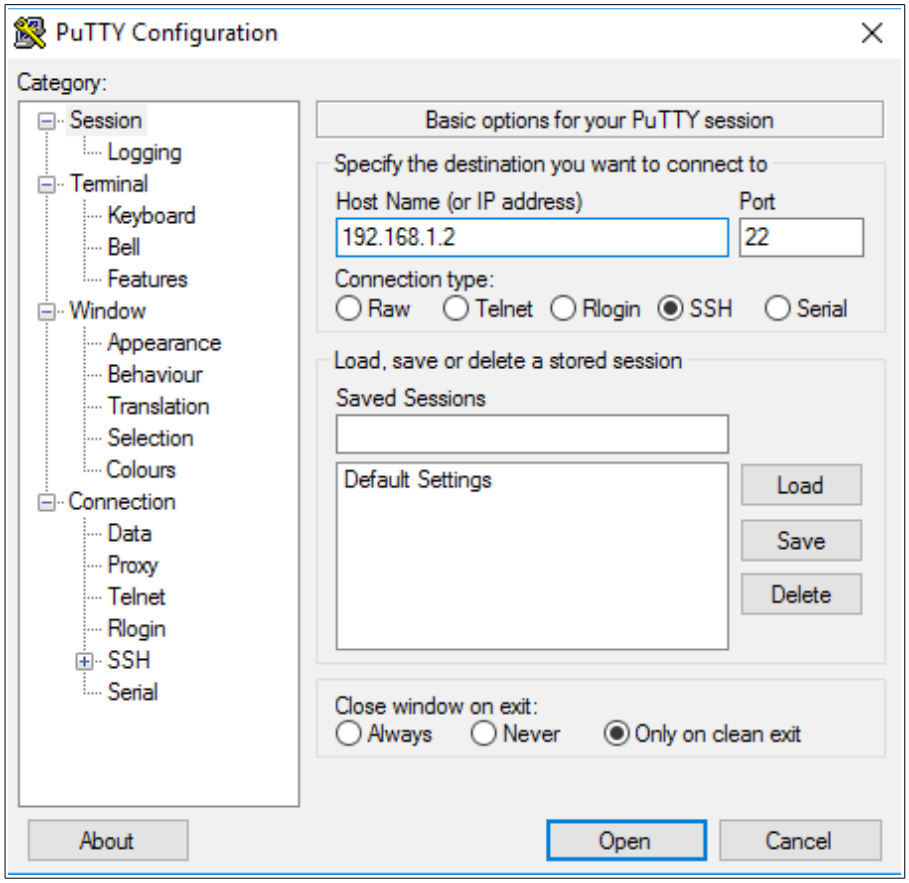

We can take a look to the listening port 22, the different private keys or the forbidden access to the root (**PermitRootLogin prohibit-password**).

Now we are going to try to connect from *linuxclient* or *windowsserver* to *linuxserver*. For that, we need to download the client Putty from the web page:

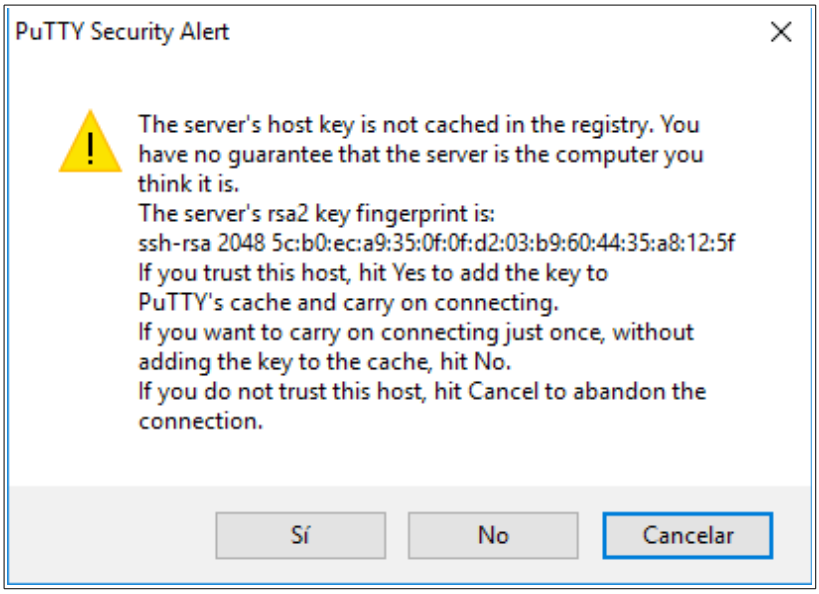
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

we are going to choose the option **putty.exe** and install it (it is easy, just follow the wizard leaving everything by default).

Once installed, we are going to try connect it to *linuxserver* (192.168.1.2) in port 22:




Then, the server will send its key fingerprint:




Now, we are going to check if that fingerprint is the same as our server. For that we write in the terminal: **ssh-keygen -l -E MD5 -f /etc/ssh/ssh_host_rsa_key.pub**

```
administrador@LinuxServer:/$ ssh-keygen -l -E MD5 -f /etc/ssh/ssh_host_rsa_key.pub
2048 MD5:5c:b0:ec:a9:35:0f:0f:d2:03:b9:60:44:35:a8:12:5f root@LinuxServer (RSA)
```

We can check that it is the same, so we click on ***YES***. The client stores the fingerprint and it will not show the alert again.
Finally, we access with the user *user*: