

UNIT 2. TO KNOW MORE ACTIVITY

Web Applications Deployment
CFGS DAW

Important: the content of this activity is not for exam

License



Attribution - NonCommercial - ShareAlike (by-nc-sa): You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may not use the material for commercial purposes. If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Nomenclature

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

This symbols are:



Important



Attention



Interesting

INDEX

1.Introduction.....	4
2.DNS.....	4
2.1 Installing and configuring cache-only DNS server in WS2016.....	4
2.1.1 Installing the DNS server.....	4
2.1.2 Configuring the DNS server.....	18
2.2 Configuring DNS server in WS2016 (primary, forward lookup zone).....	19
2.2.1 Configuring the DNS suffix.....	20
2.2.2 Configuring the forward lookup zone.....	21
2.3 Configuring DNS server in WS2016 (primary, reverse lookup zone).....	35
2.3.1 Configuring the reverse lookup zone.....	35
2.4 Configuring DNS server in Linux.....	48
2.4.1 Installing the server.....	48
2.4.2 Configuring the forward and reverse lookup zone.....	49
2.5 Configuring the client.....	54
3.FTP.....	55
3.1 Installing FTP server.....	55
3.2 Configuring FTP server.....	56
4.SSH.....	61
4.1 Installing SSH server.....	61
4.2 Configuring SSH server.....	62

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

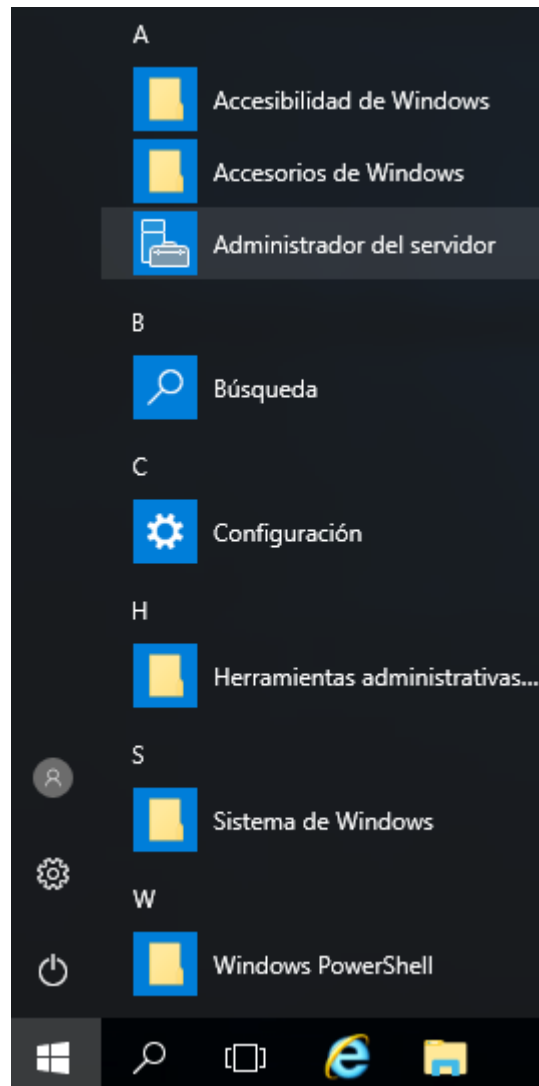
2.1 Installing and configuring cache-only DNS server in WS2016

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.

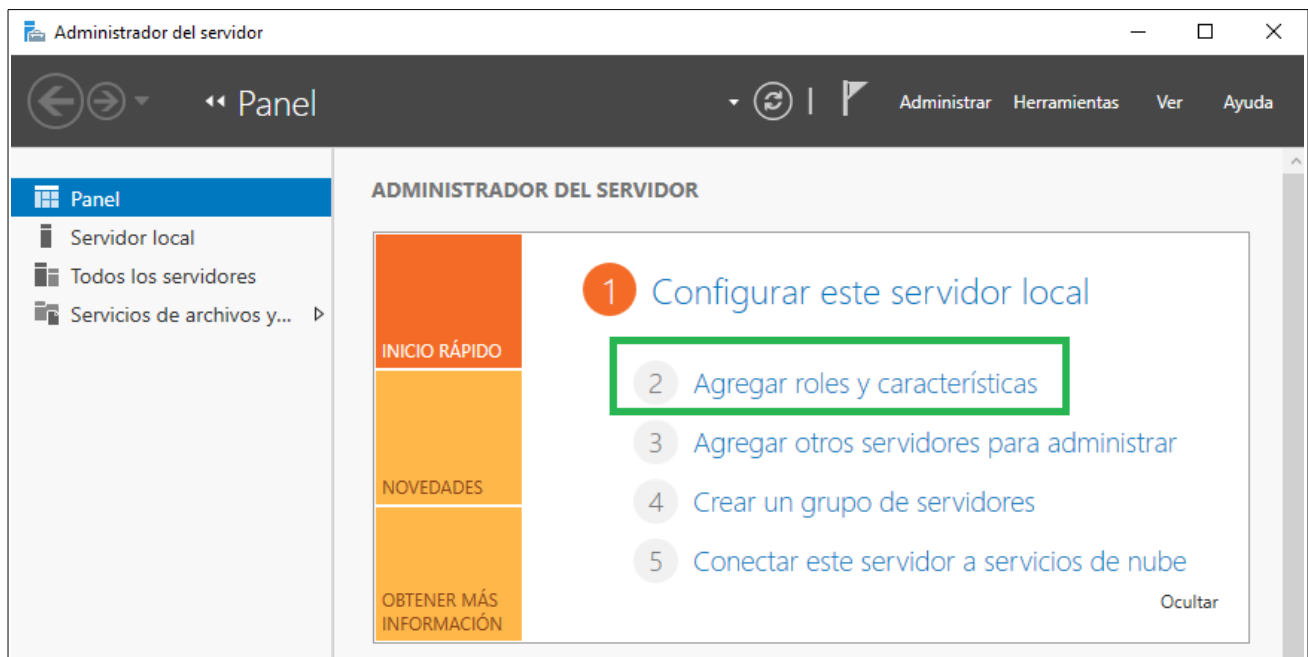
2.1.1 Installing the DNS server

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

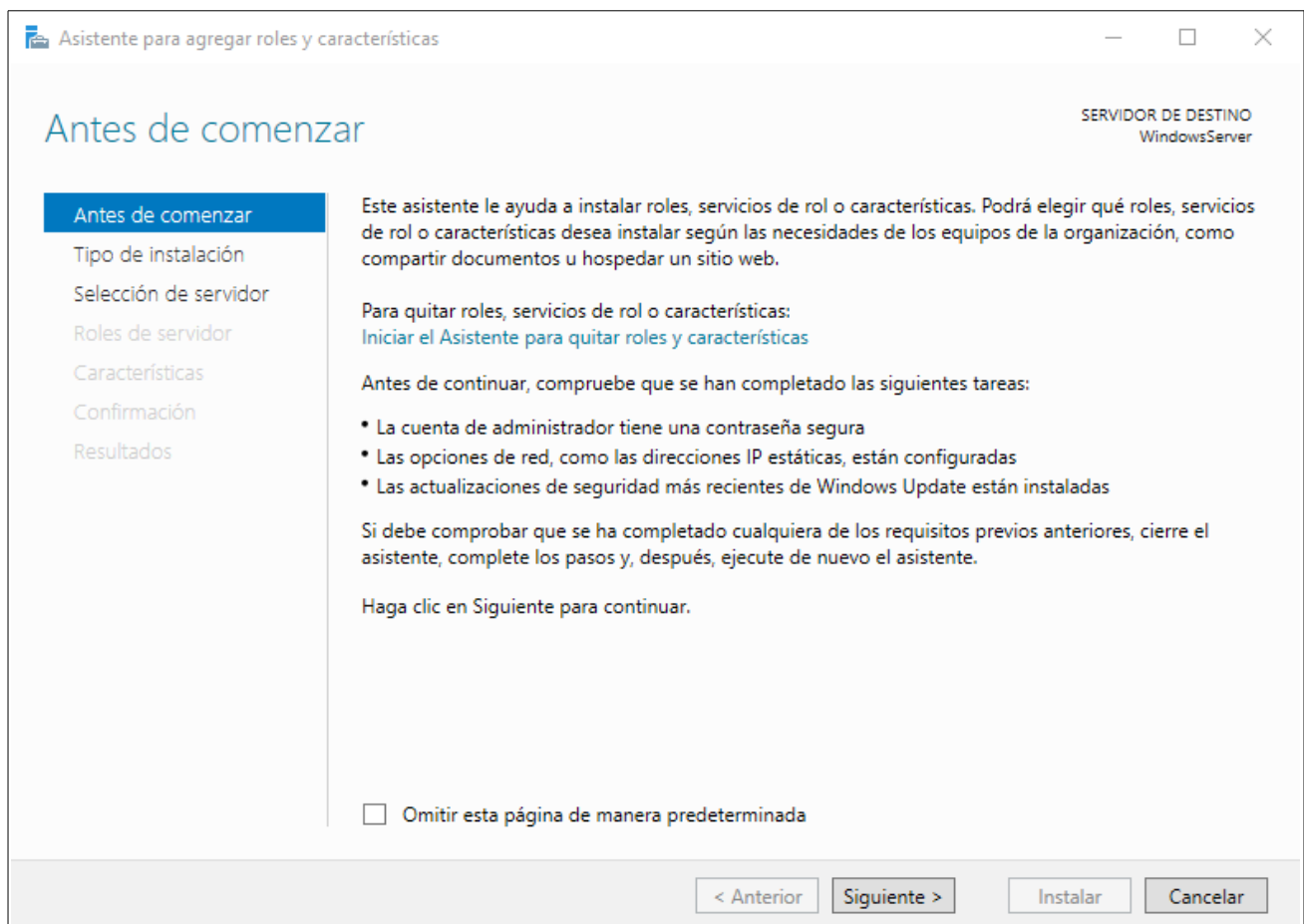
1. Start session at *windowsServer* virtual machine with the administrator user.
2. Click on **START MENU > SERVER MANAGER**



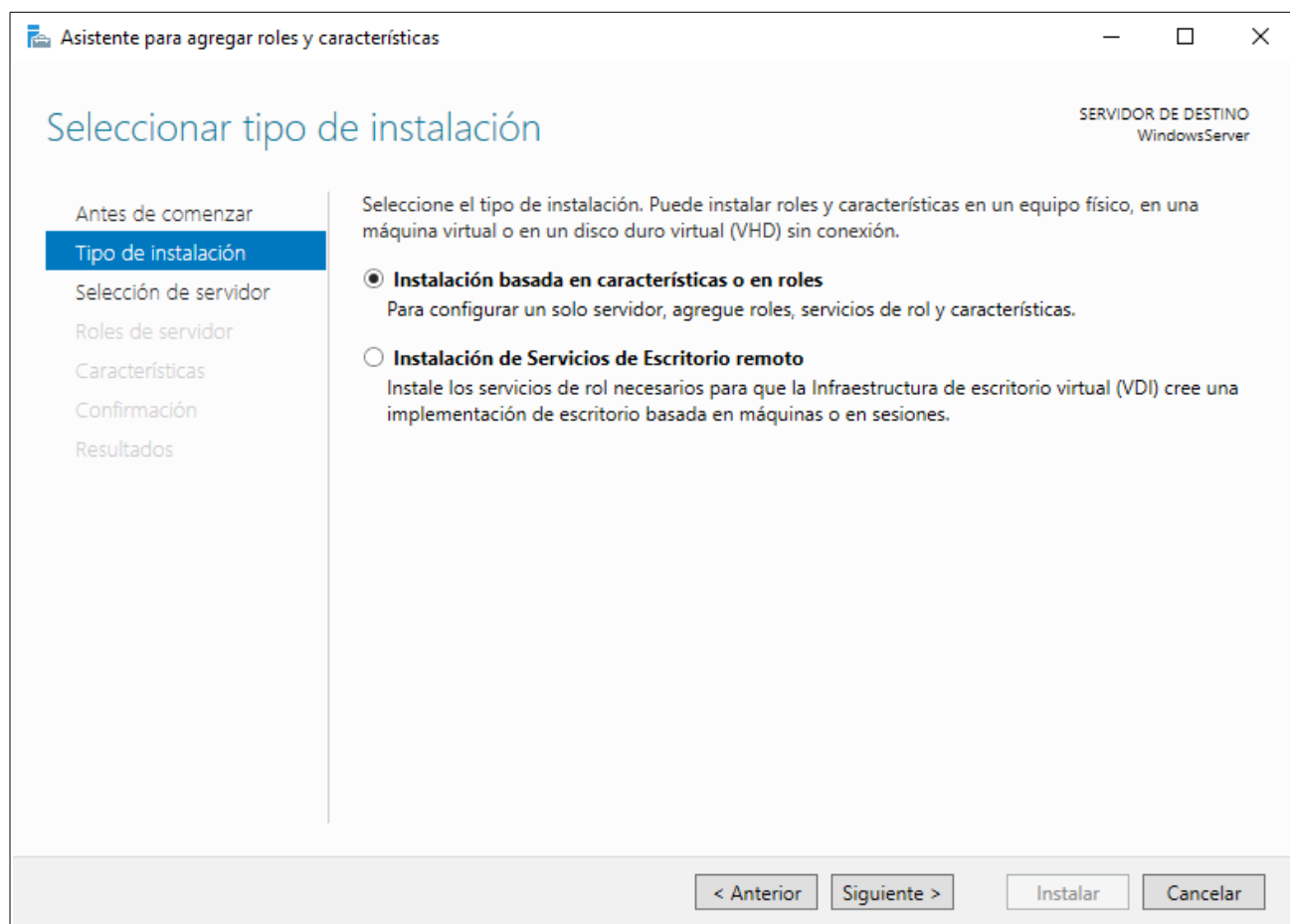
3. On the left, click on **ADD ROLES AND FEATURES**



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**

Asistente para agregar roles y características

Seleccionar servidor de destino

SERVIDOR DE DESTINO
WindowsServer

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
Confirmación
Resultados

Seleccione un servidor o un disco duro virtual en el que se instalarán roles y características.

☒ Seleccionar un servidor del grupo de servidores
☐ Seleccionar un disco duro virtual

Grupo de servidores

Filtro:

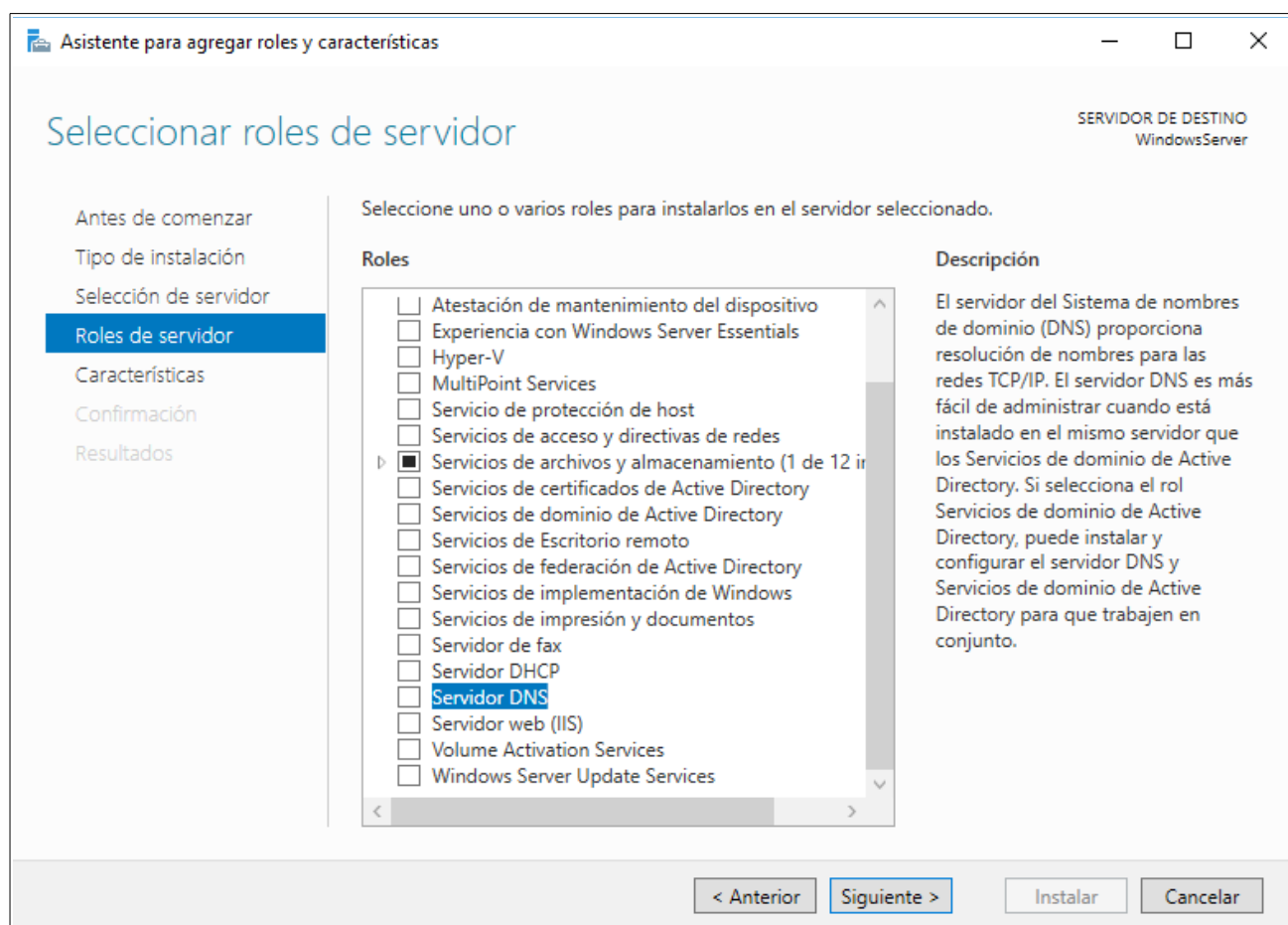
Nombre	Dirección IP	Sistema operativo
WindowsServer	192.168.1.3	Microsoft Windows Server 2016 Standard Evaluation

1 equipo(s) encontrado(s)

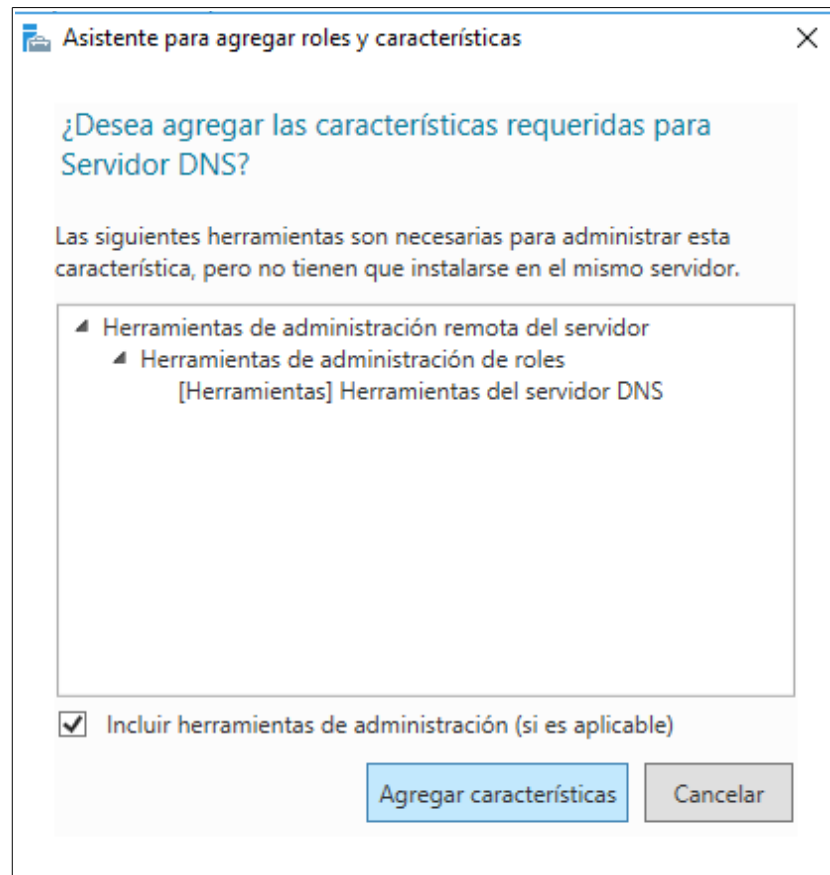
Esta página muestra los servidores que ejecutan Windows Server 2012 o una versión más reciente de Windows Server, y que se agregaron mediante el comando Agregar servidores del Administrador del servidor. No se muestran los servidores sin conexión ni los servidores recién agregados para los que la recopilación de datos aún está incompleta.

< Anterior Siguiente > Instalar Cancelar

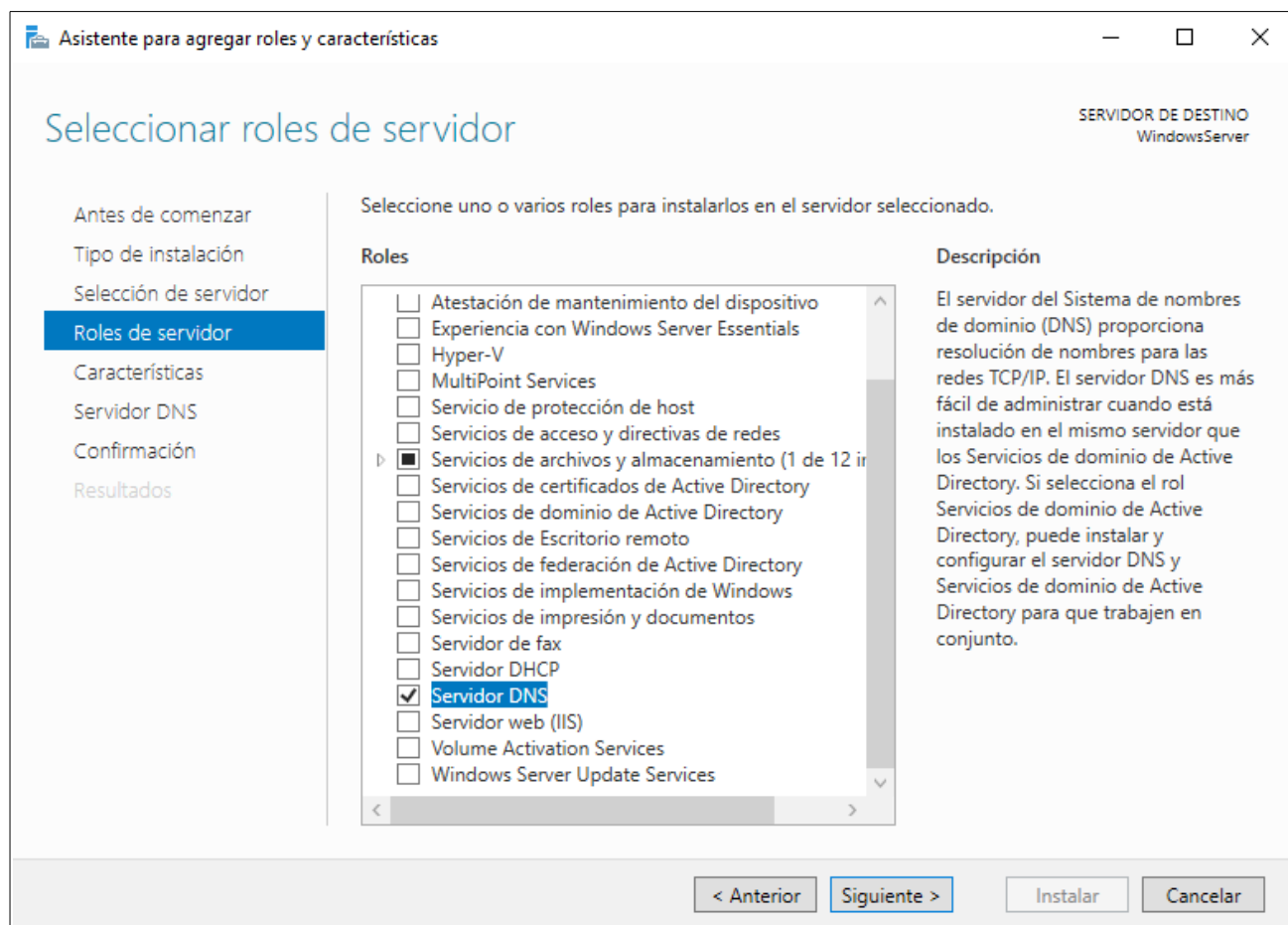
7. Select **DNS SERVER** and click on **NEXT**



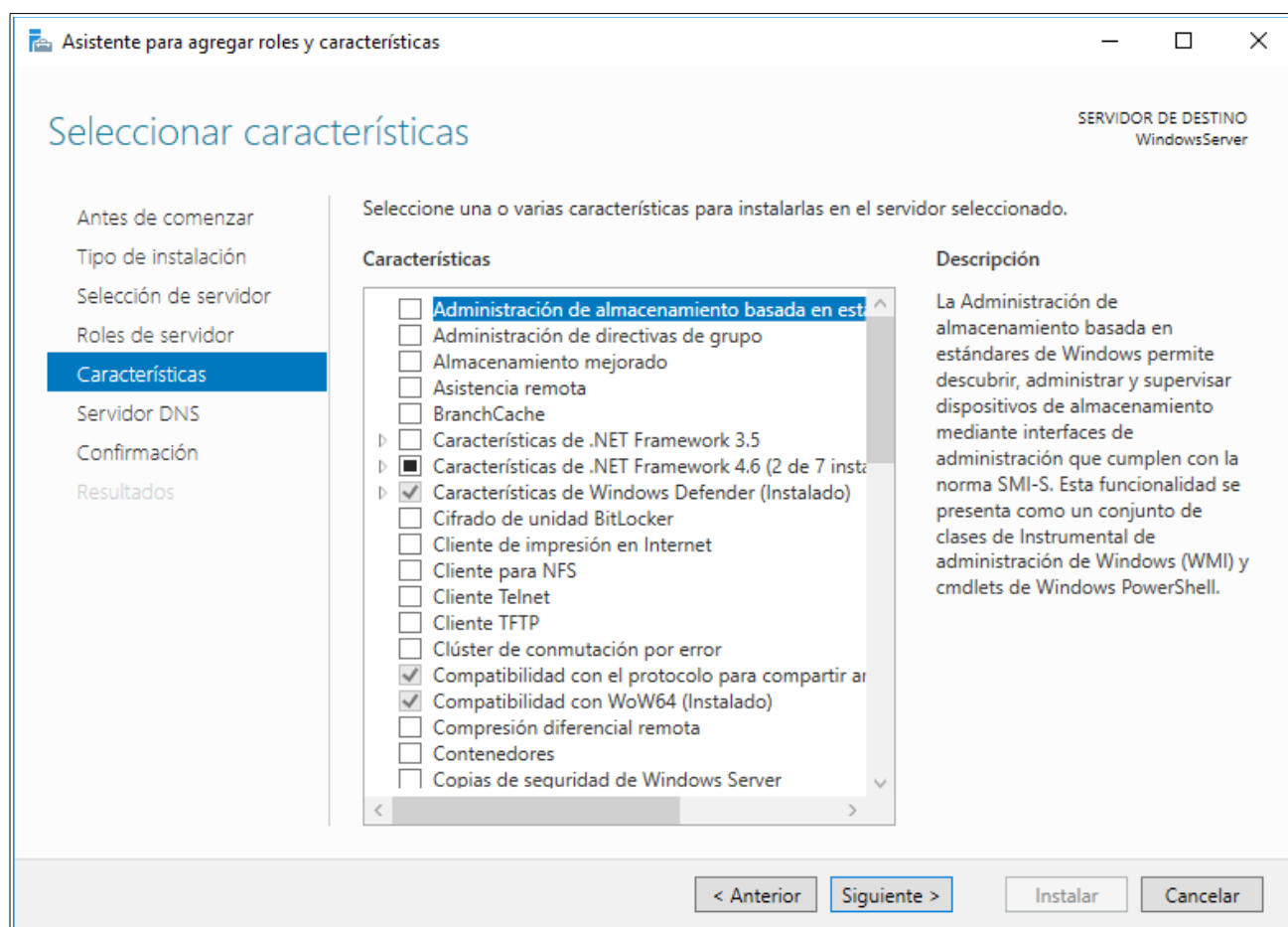
8. Click on **ADD FEATURES**



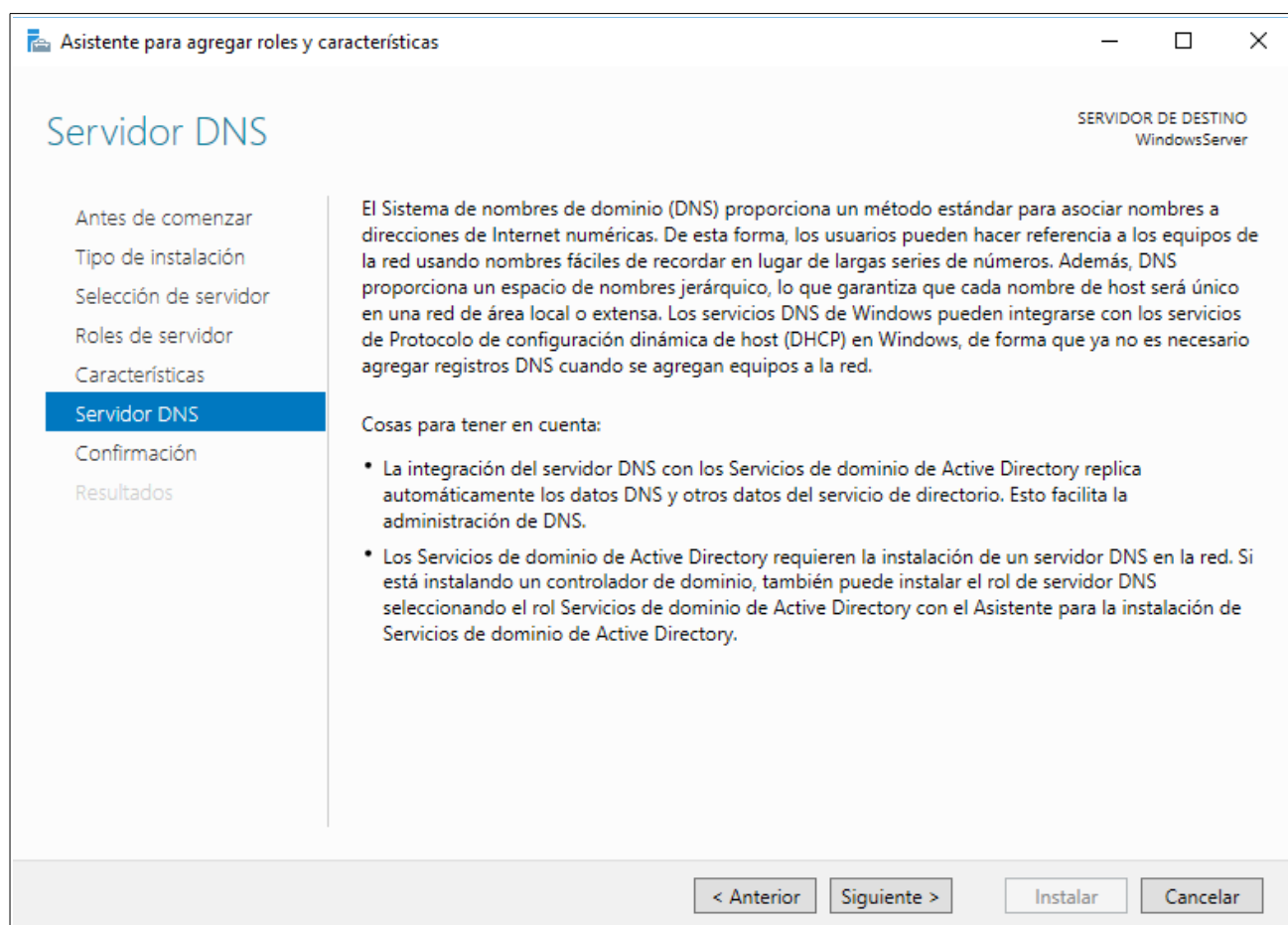
9. Click on **NEXT**



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)

Asistente para agregar roles y características

SERVIDOR DE DESTINO
WindowsServer

Confirmar selecciones de instalación

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
Servidor DNS
Confirmación
Resultados

Para instalar los siguientes roles, servicios de rol o características en el servidor seleccionado, haga clic en Instalar.

☐ Reiniciar automáticamente el servidor de destino en caso necesario

En esta página se pueden mostrar características opcionales (como herramientas de administración) porque se seleccionaron automáticamente. Si no desea instalar estas características opcionales, haga clic en Anterior para desactivar las casillas.

Herramientas de administración remota del servidor

Herramientas de administración de roles

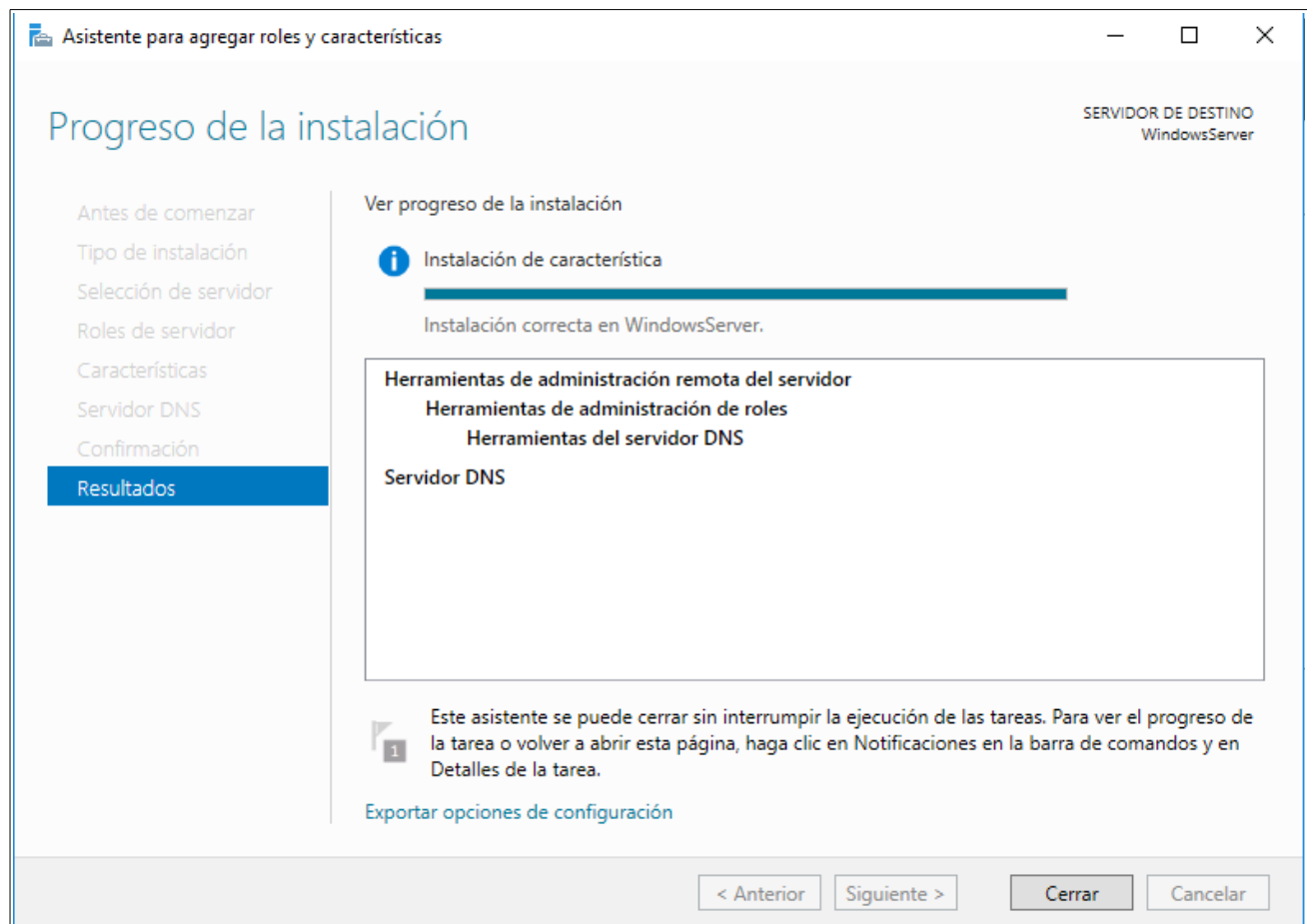
Herramientas del servidor DNS

Servidor DNS

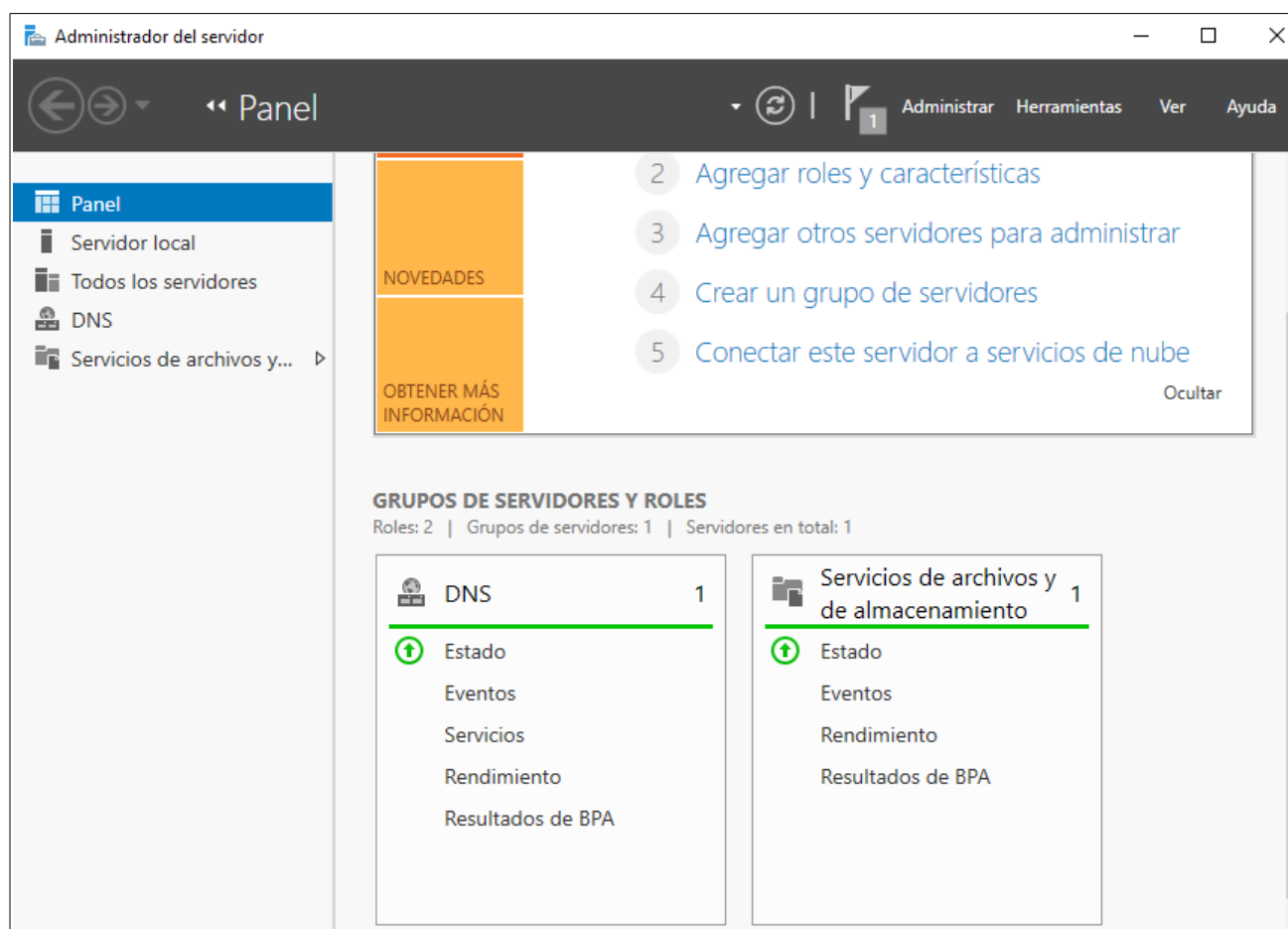
[Exportar opciones de configuración](#)
Especifique una ruta de acceso de origen alternativa

< Anterior Siguiendo > Instalar Cancelar

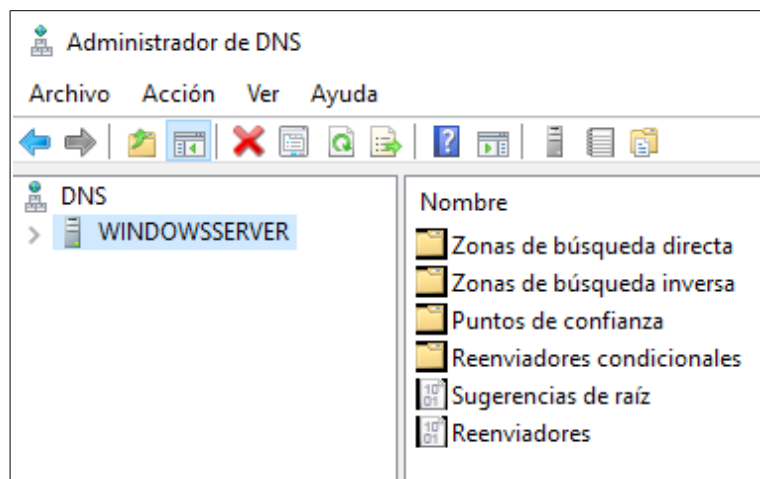
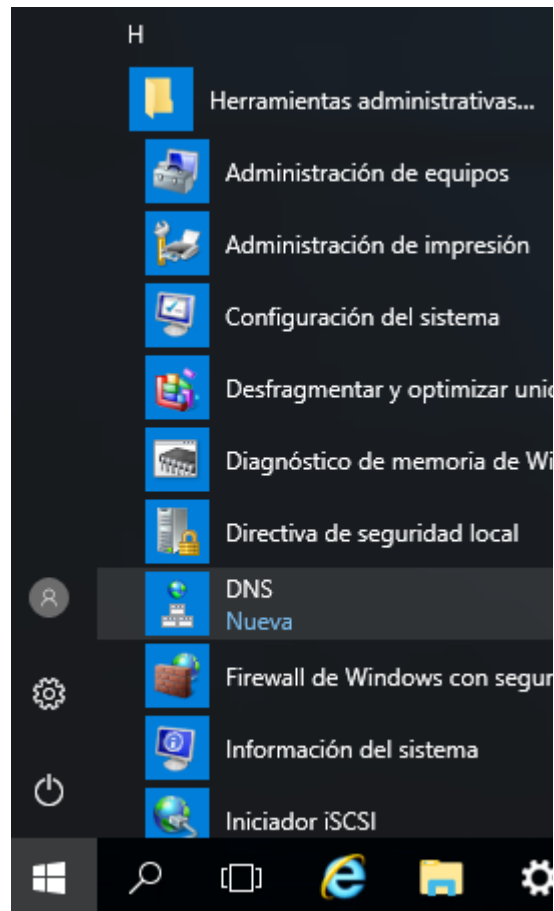
13. And the installation will be completed. Click on **CLOSE**



We can see it in the Panel



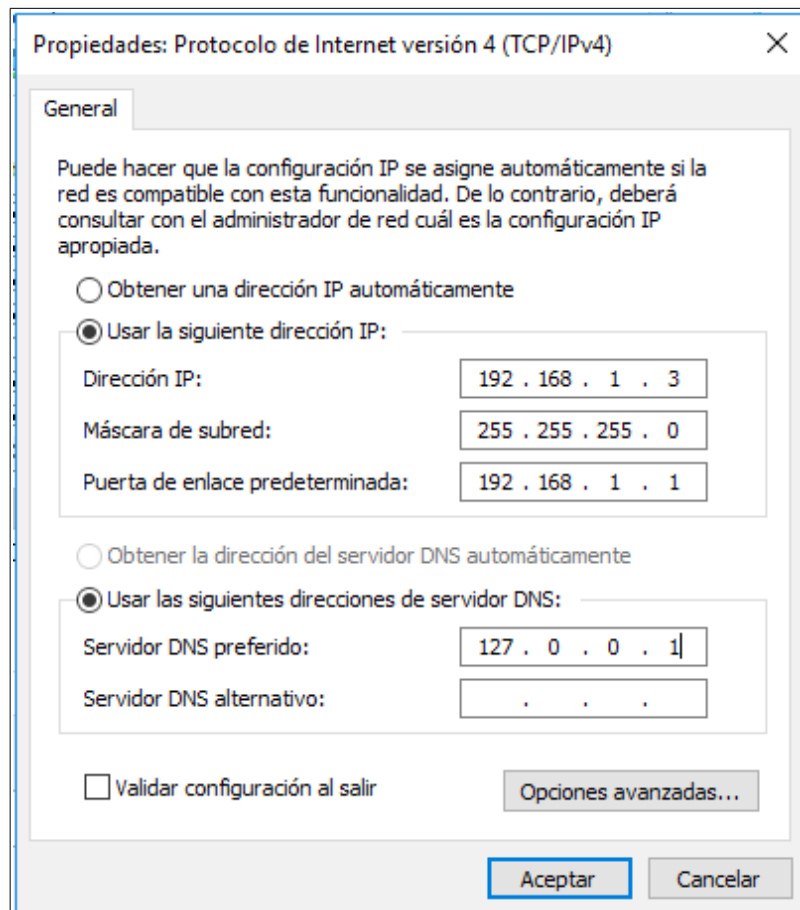
We can check that the DNS server is installed clicking on **START MENU > ADMINISTRATIVE TOOLS > DNS**



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):

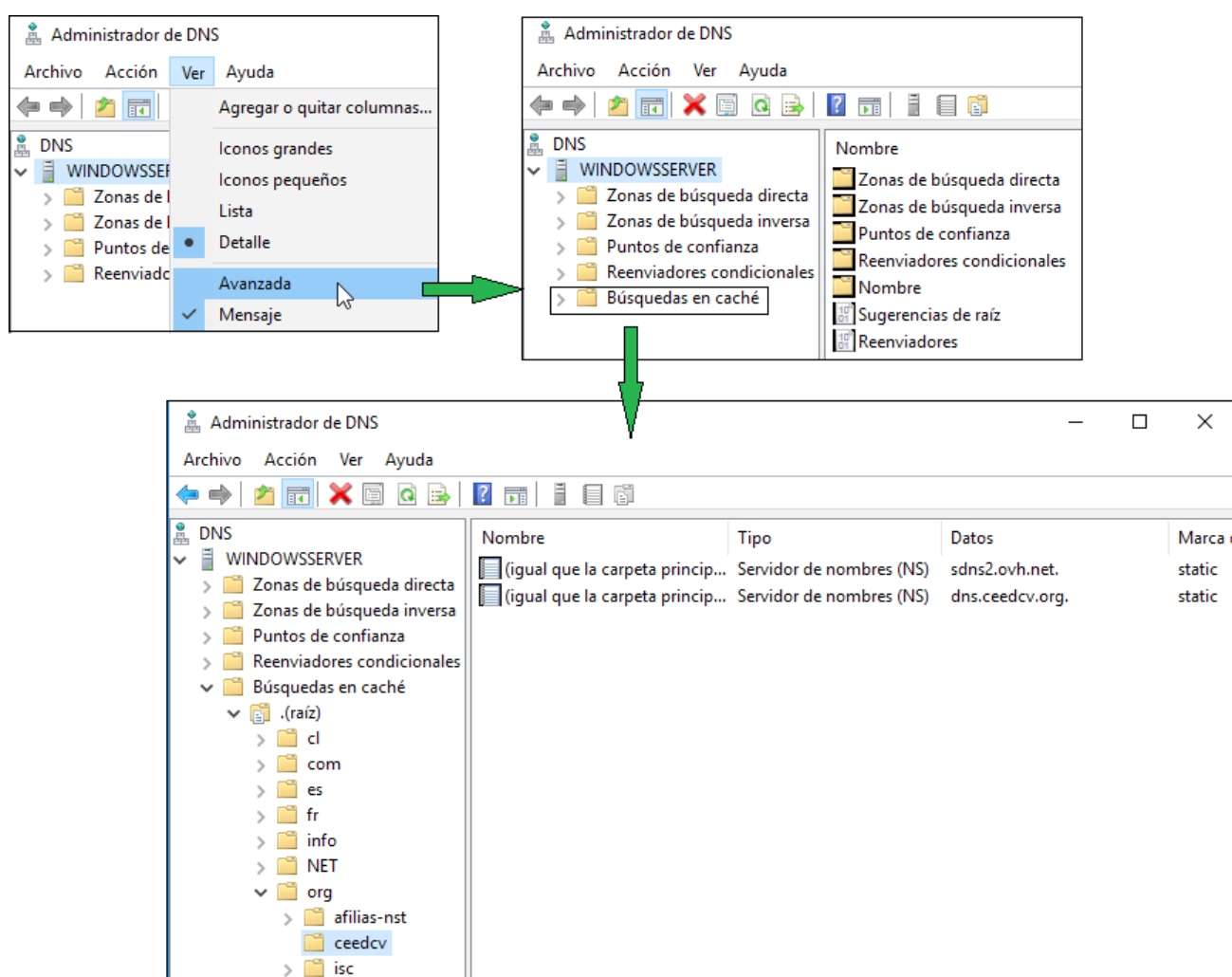


Then we will use the nslookup command to resolve a name, for instance www.ceedcv.org:

```
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)

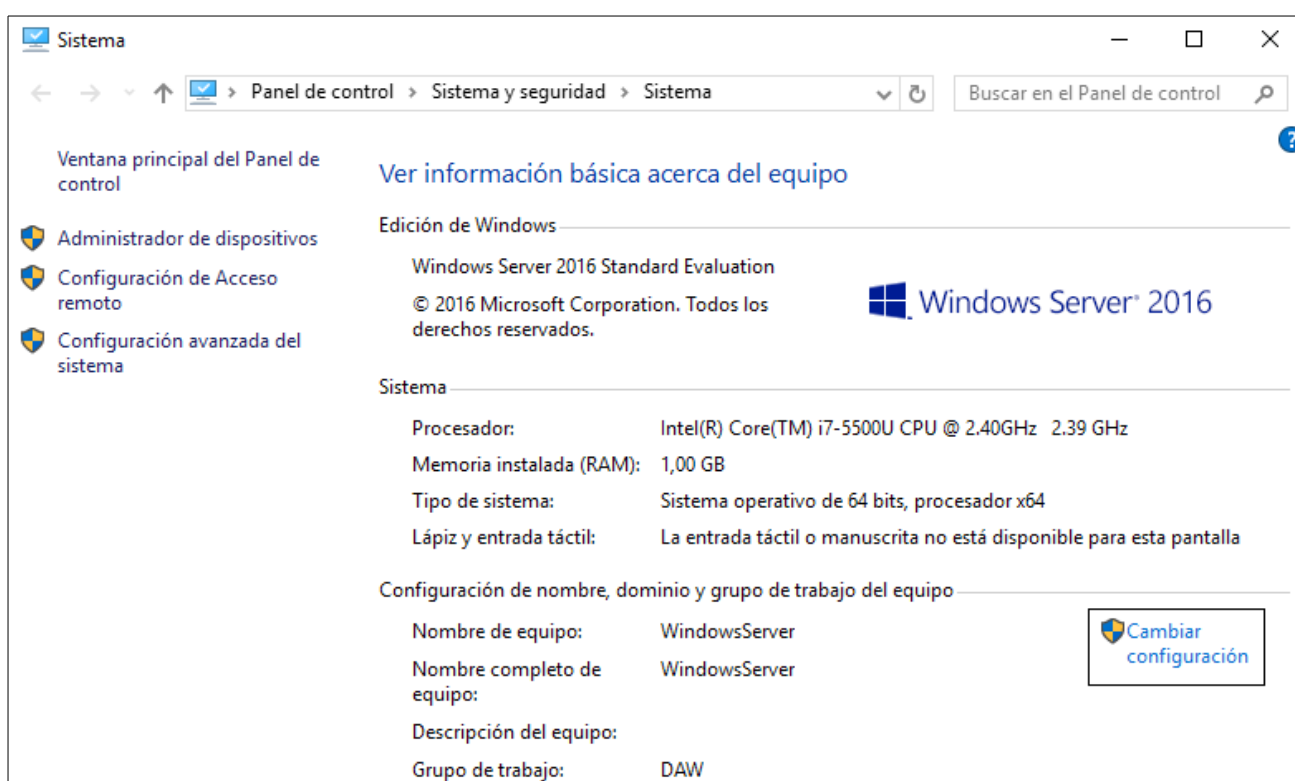
Now we are going to configure the DNS server as primary to a forward lookup zone, so in this case:

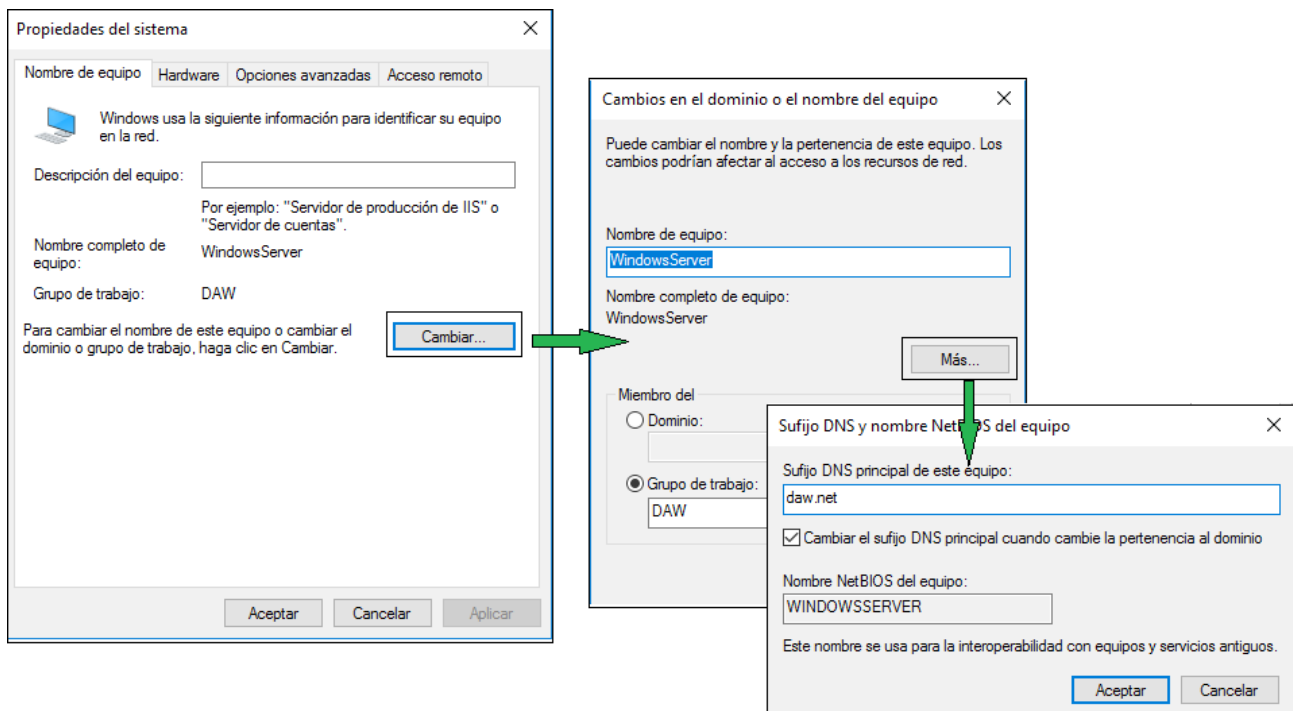
- The server will only works to the local network (not to hosts from Internet)
- The server will works as master (primary) and it will have authority to the domain *daw.net*:

- 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**

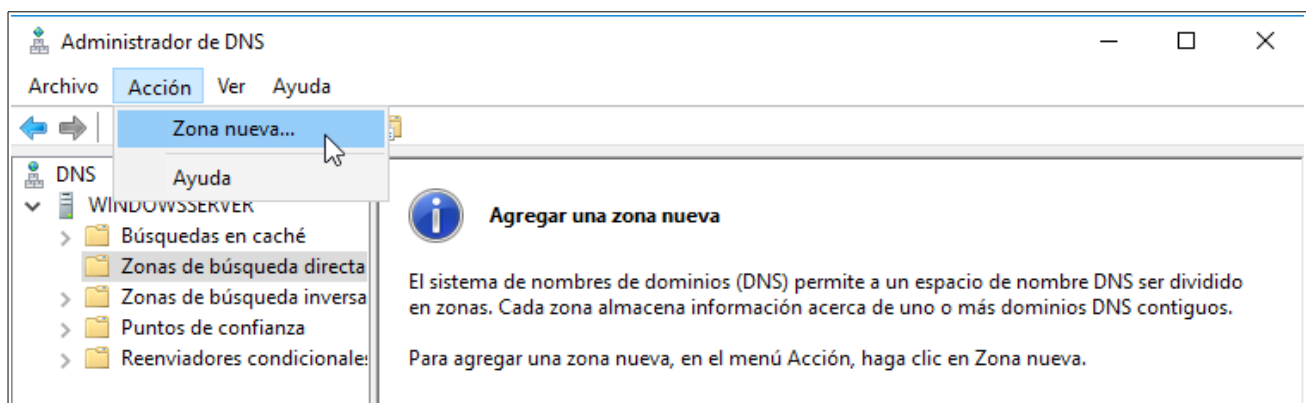




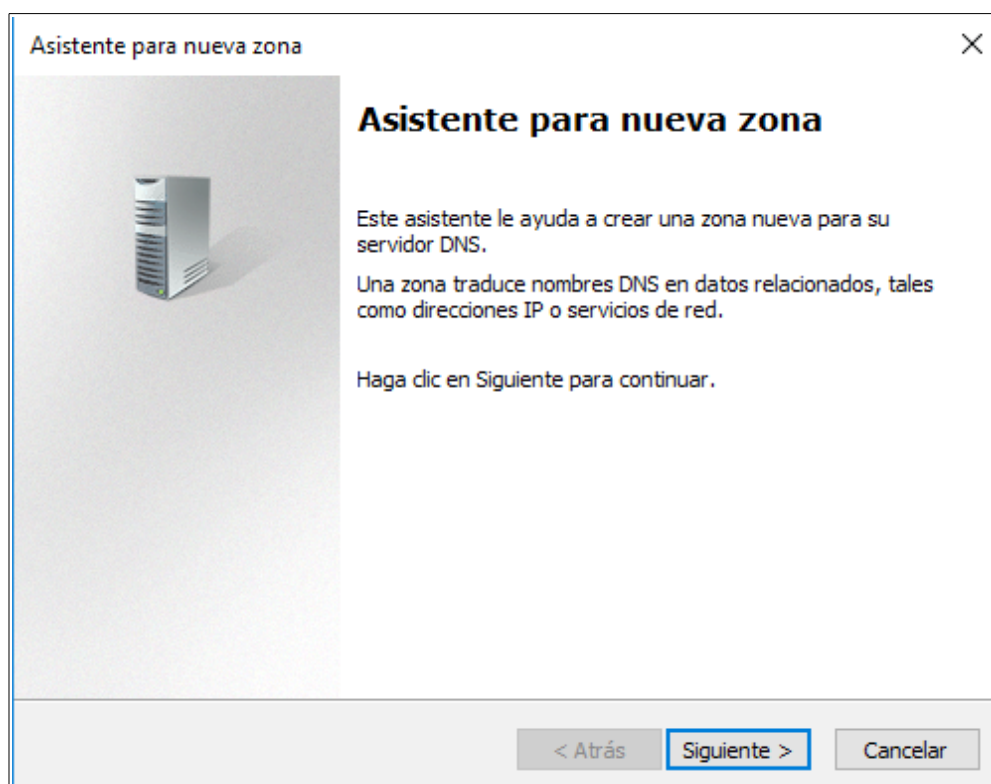
2.2.2 Configuring the forward lookup zone

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

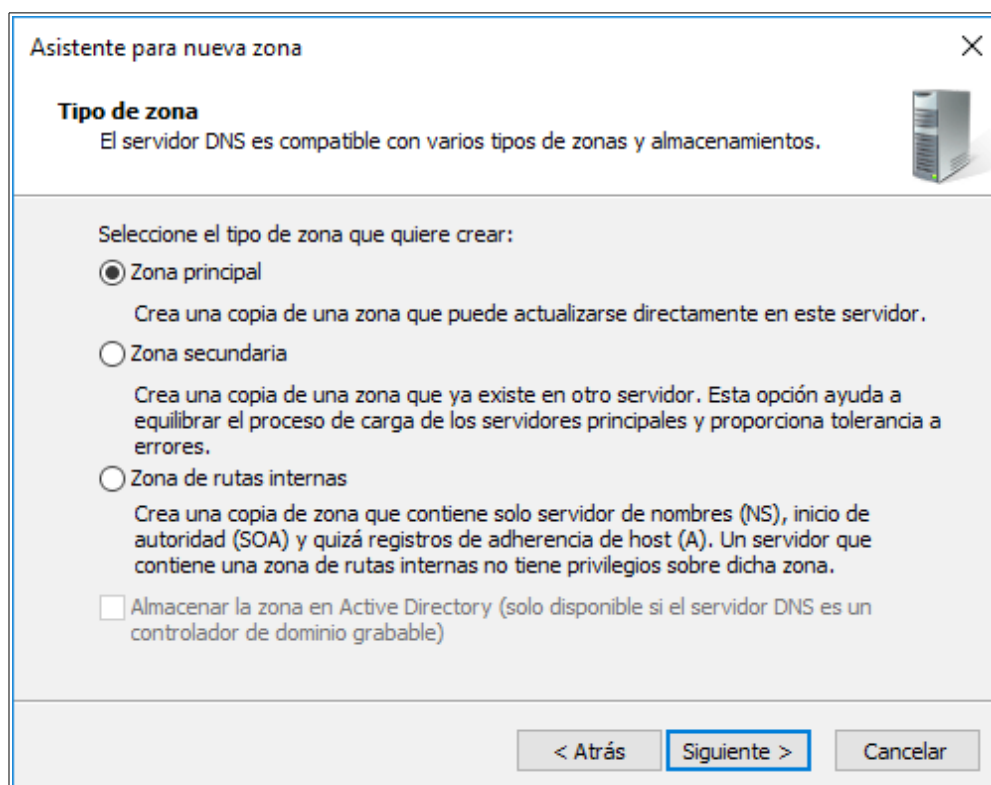
1. Go to the server administration window, select **FORWARD LOOKUP ZONE** and click on **ACTION** and **NEW ZONE**



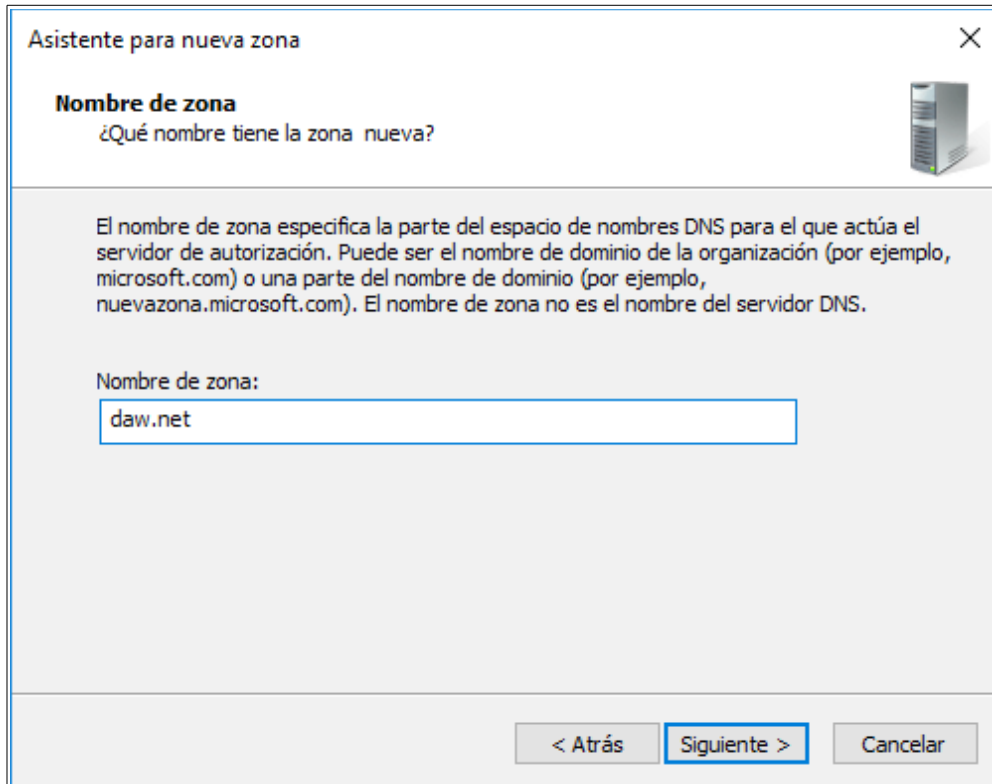
2. Read the information of the wizard and click on **NEXT**



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



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



Asistente para nueva zona

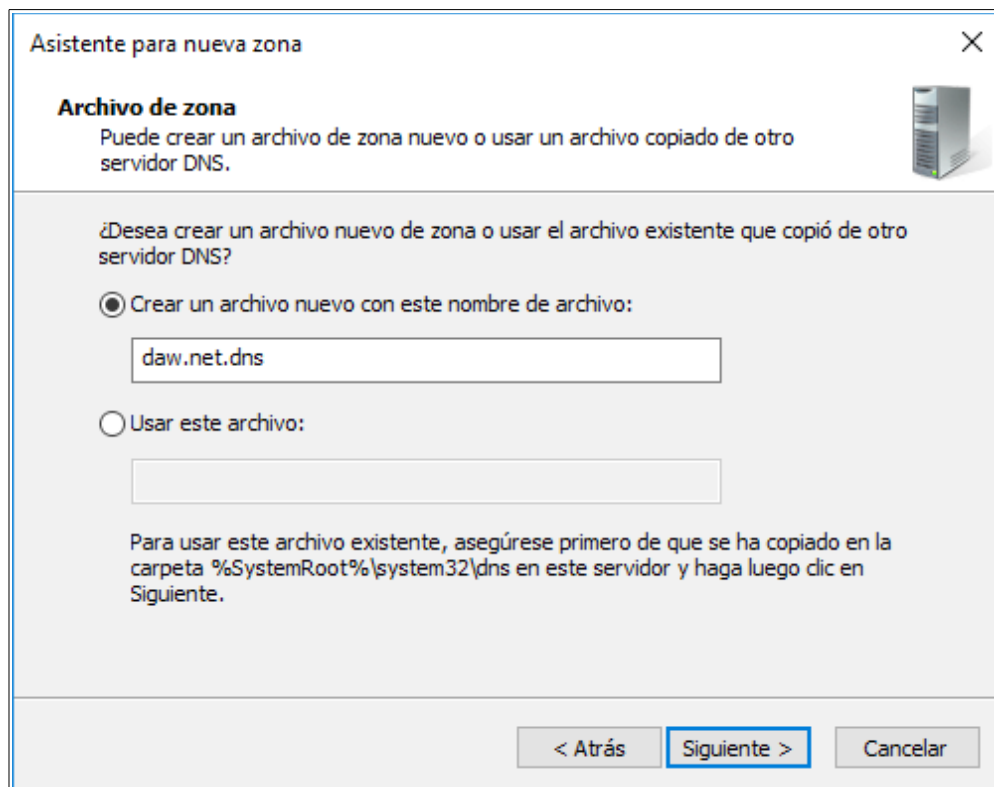
Nombre de zona
¿Qué nombre tiene la zona nueva?

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:
daw.net

< Atrás **Siguiete >** Cancelar

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**


Asistente para nueva zona

Actualización dinámica

Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.

Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.

Seleccione el tipo de actualizaciones dinámicas que desea permitir:

- ☐ Permitir solo actualizaciones dinámicas seguras (recomendado para Active Directory)
Esta opción solo está disponible para las zonas que están integradas en Active Directory.
- ☐ Permitir todas las actualizaciones dinámicas (seguras y no seguras)
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
 Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.
- ☒ No admitir actualizaciones dinámicas
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.

< Atrás **Siguiente >** Cancelar

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

Asistente para nueva zona

Finalización del Asistente para nueva zona

Se ha completado correctamente el Asistente para nueva zona. Ha especificado la siguiente configuración:

Nombre: daw.net

Tipo: Primaria estándar

Tipo de búsqueda: Reenviar

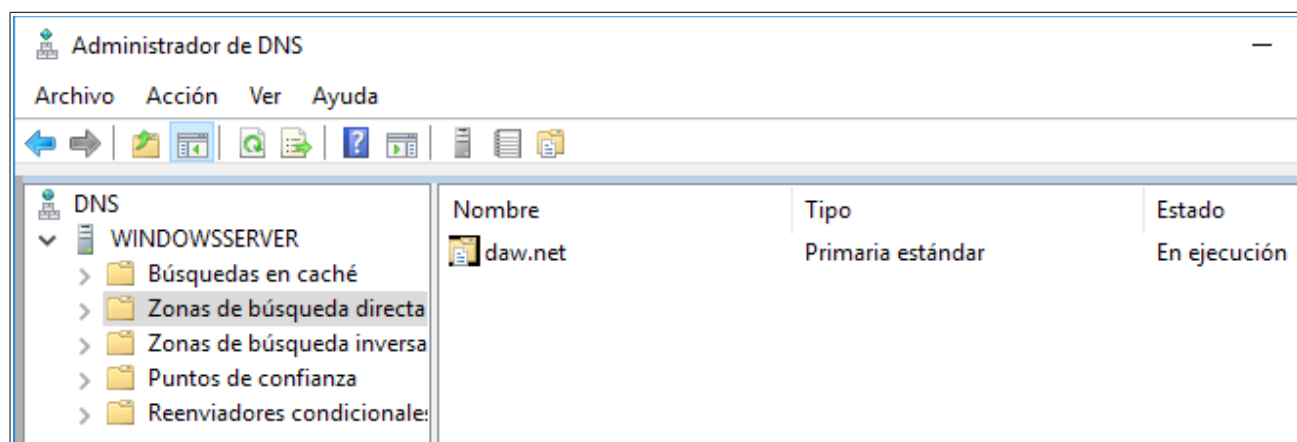
Nombre de archivo: daw.net.dns

Nota: ahora debe agregar registros a la zona o asegurarse de que los registros se actualizan dinámicamente. A continuación, compruebe la resolución de nombres con nslookup.

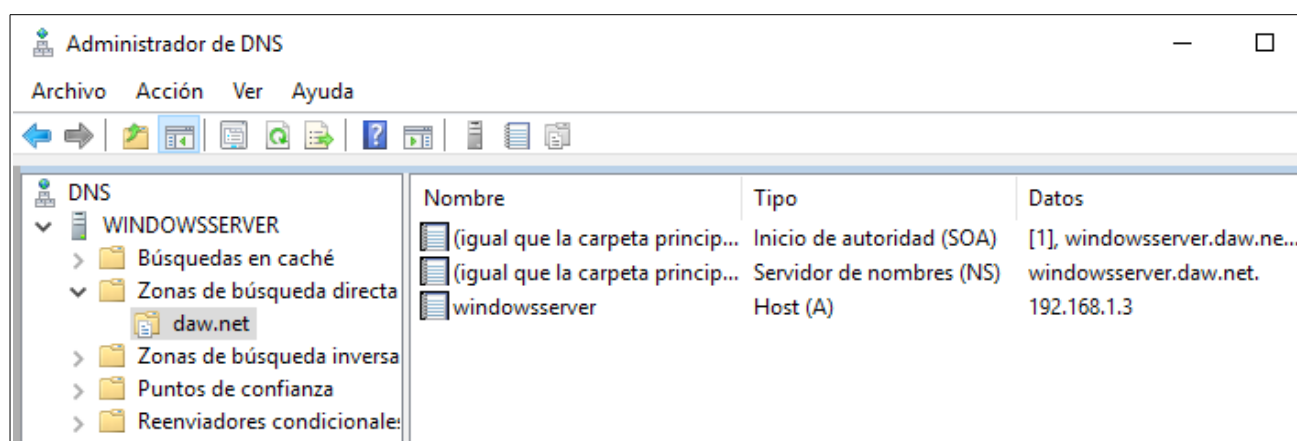
Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.

< Atrás **Finalizar** Cancelar

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.

Propiedades de daw.net

Servidores de nombres WINS Transferencias de zona

General Inicio de autoridad (SOA)

Número de serie: 1 Incremento

Servidor principal: windowsserver.daw.net Examinar...

Persona responsable: hostmaster.daw.net Examinar...

Intervalo de actualización: 15 Minutos

Intervalo de reintento: 10 Minutos

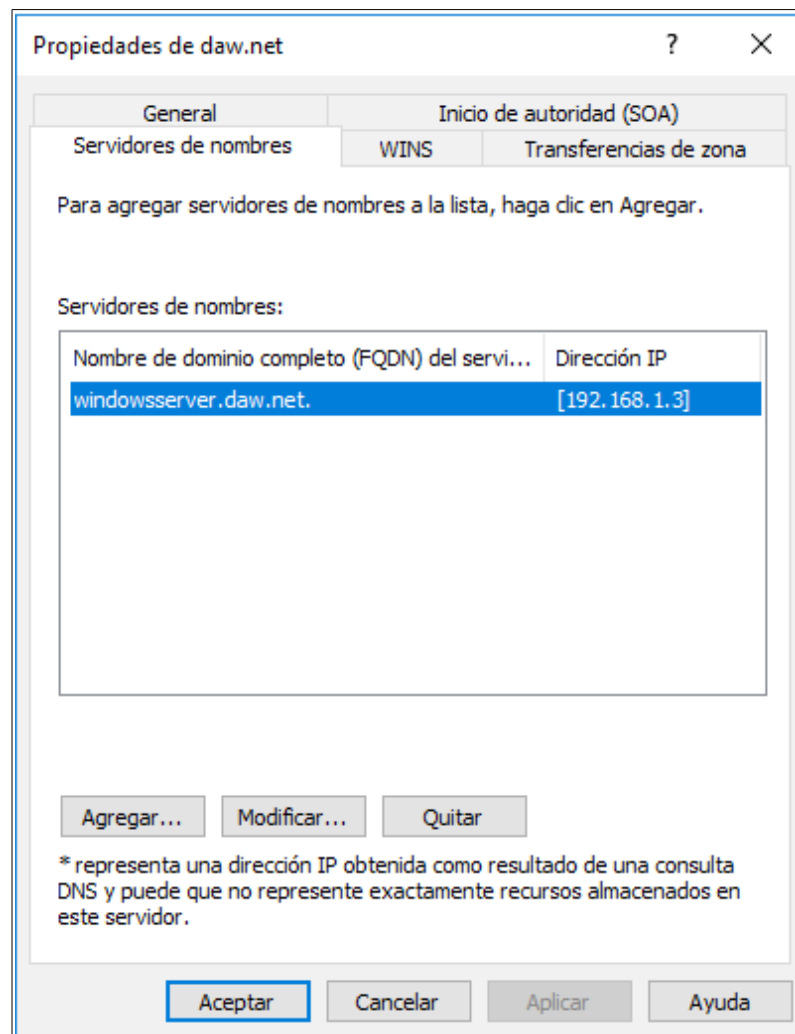
Expira después de: 1 Días

TTL mínimo (predeterminado): 1 Horas

TTL para este registro: 0 :1 :0 :0 (DDDDD:HH.MM.SS)

Aceptar Cancelar Aplicar Ayuda

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



Propiedades de windowsserver

Host (A)

Host (si se deja en blanco, se usa el nombre del dominio primario):
windowsserver

Nombre de dominio completo (FQDN):
windowsserver.daw.net

Dirección IP:
192.168.1.3

☐ Actualizar registro del puntero (PTR) asociado

☐ Eliminar este registro cuando quede obsoleto

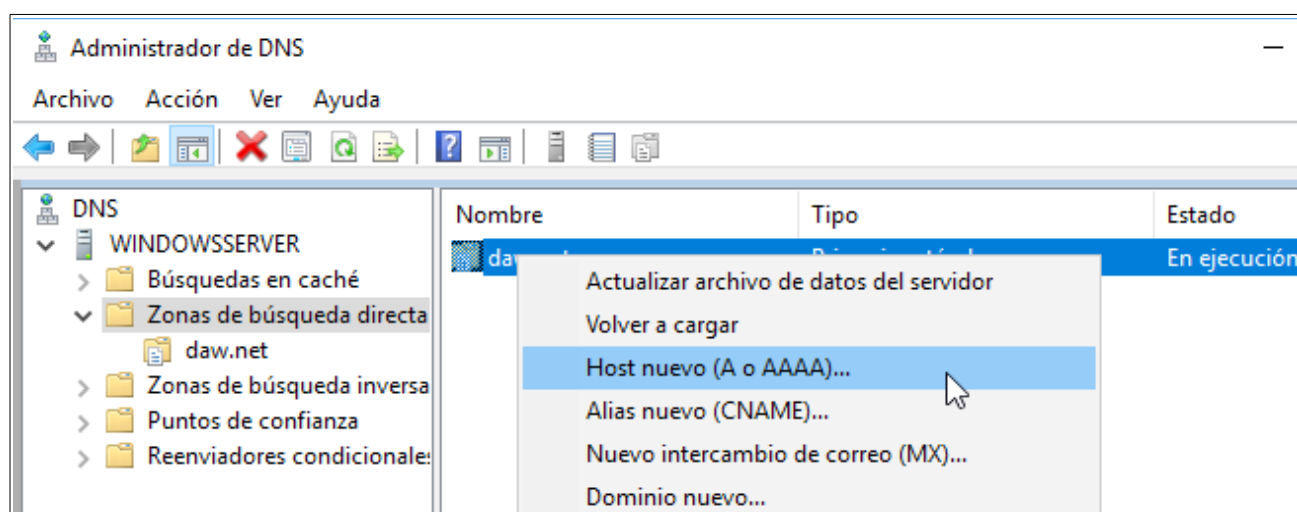
Marca de tiempo de registro:

Período de vida (TTL): 0 :1 :0 :0 (DDDD:HH.MM.SS)

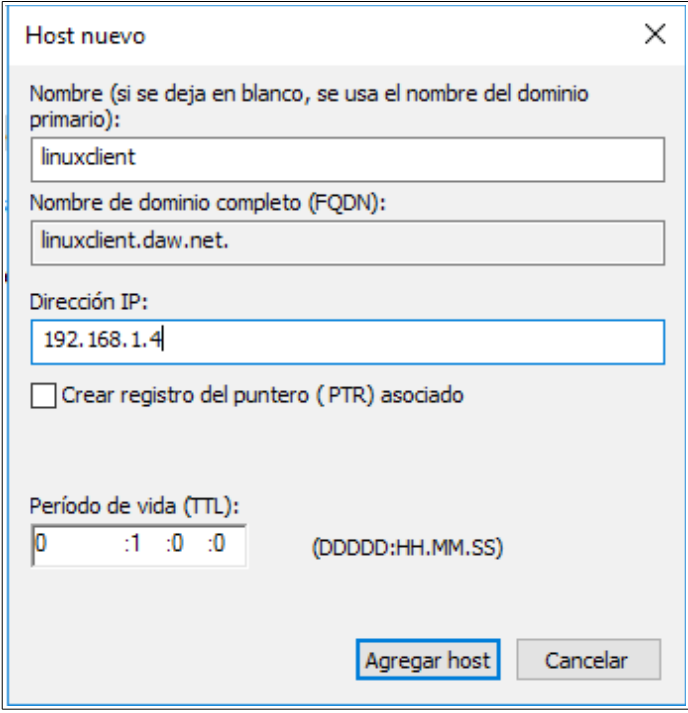
Aceptar Cancelar Aplicar

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



Host nuevo

Nombre (si se deja en blanco, se usa el nombre del dominio primario):
linuxclient

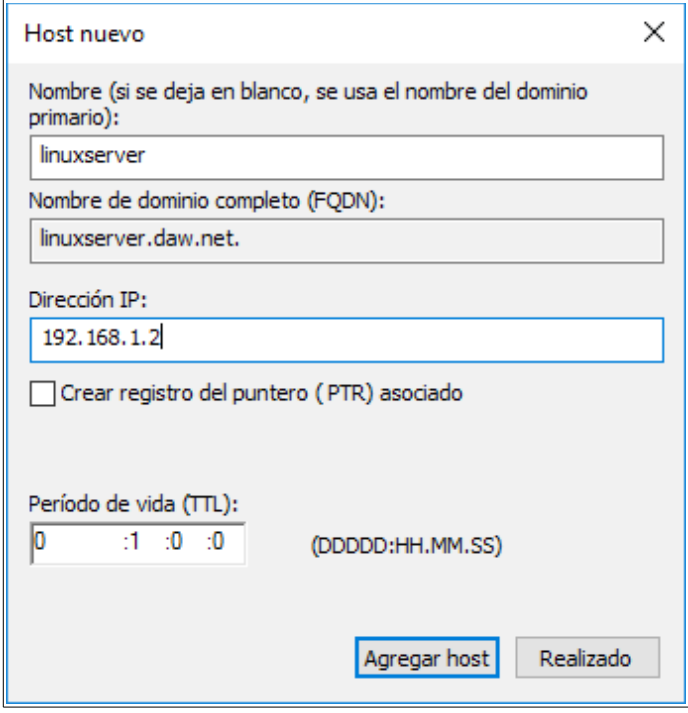
Nombre de dominio completo (FQDN):
linuxclient.daw.net.

Dirección IP:
192.168.1.4

☐ Crear registro del puntero (PTR) asociado

Período de vida (TTL):
0 :1 :0 :0 (DDDDD:HH.MM.SS)

Agregar host Cancelar



Host nuevo

Nombre (si se deja en blanco, se usa el nombre del dominio primario):
linuxserver

Nombre de dominio completo (FQDN):
linuxserver.daw.net.

Dirección IP:
192.168.1.2

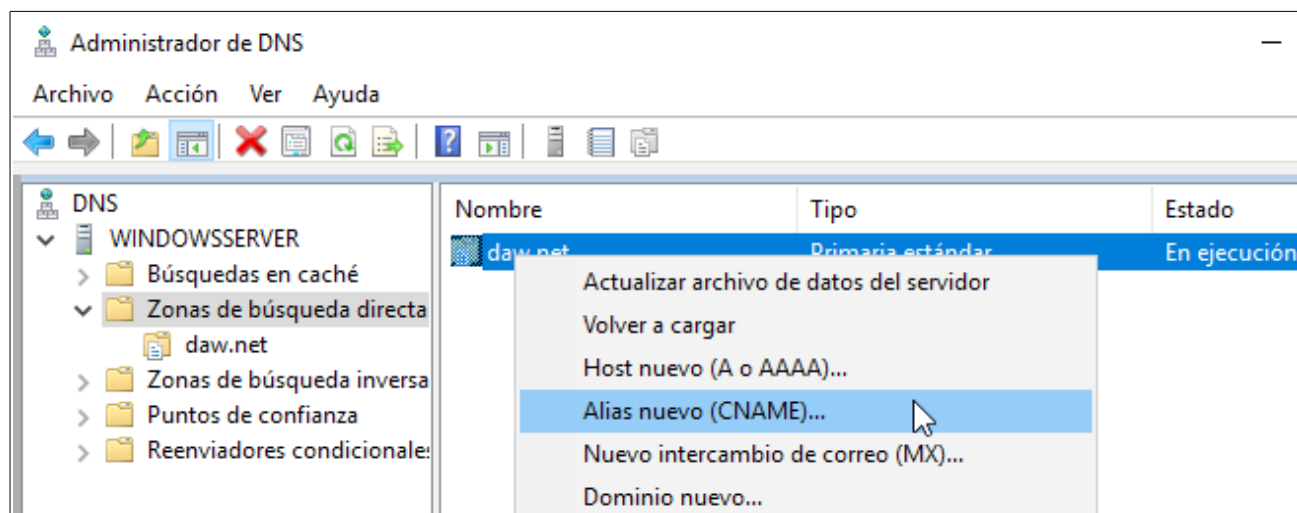
☐ Crear registro del puntero (PTR) asociado

Período de vida (TTL):
0 :1 :0 :0 (DDDDD:HH.MM.SS)

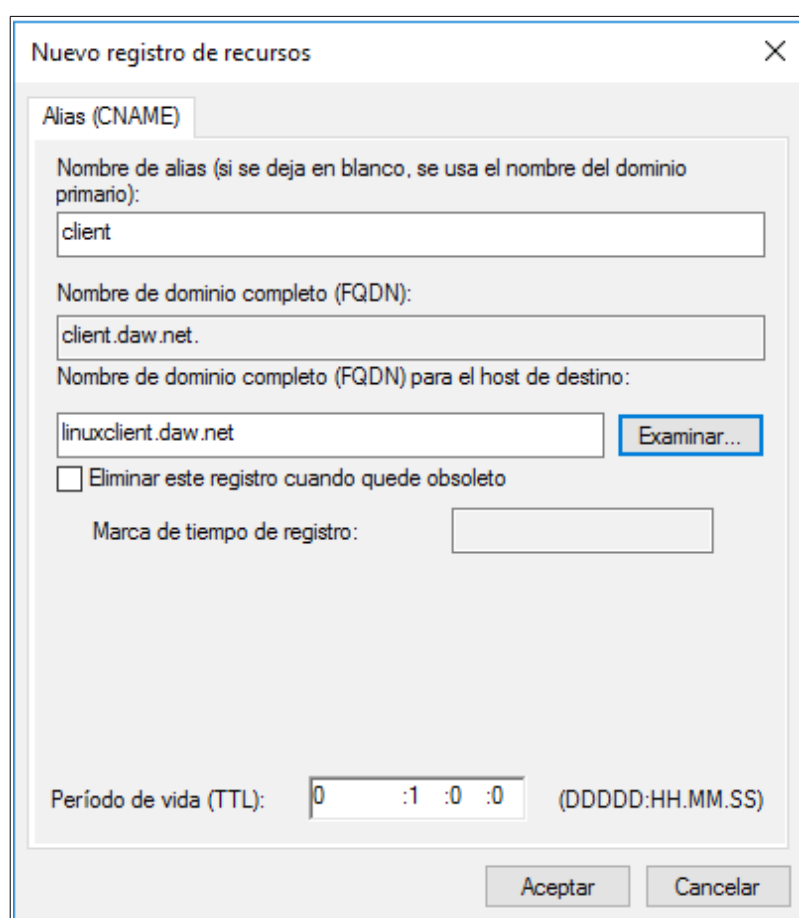
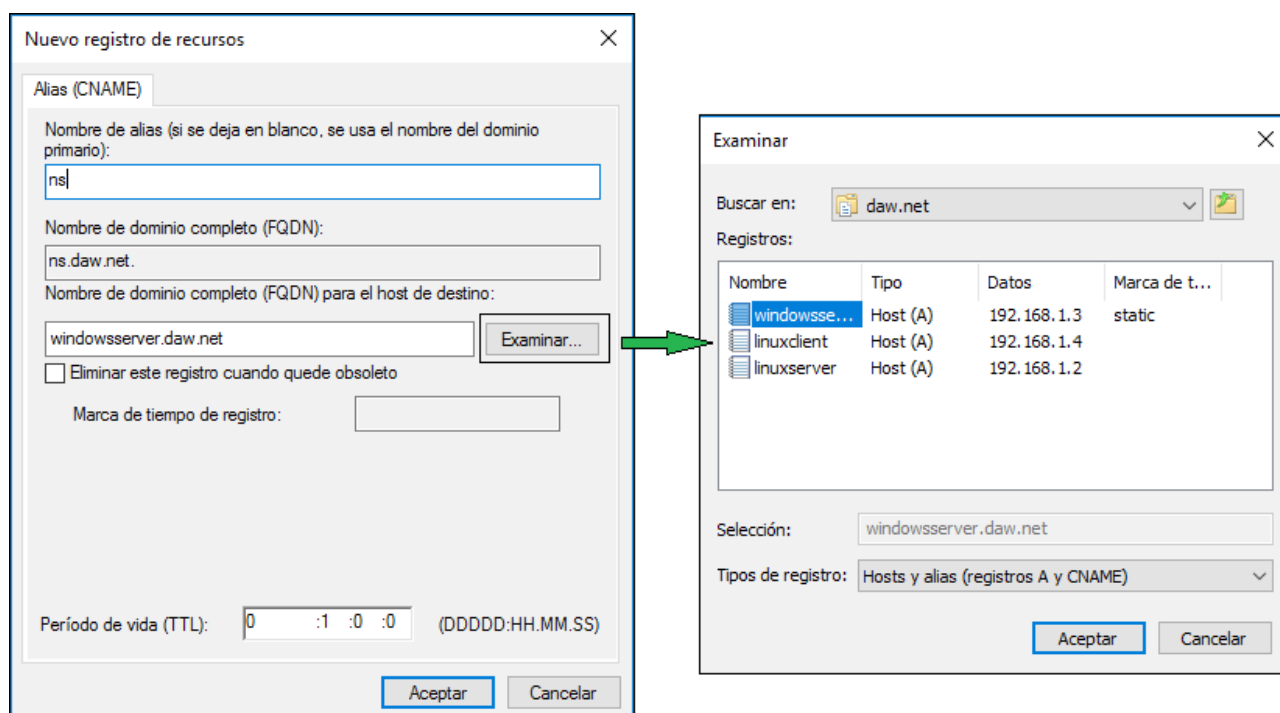
Agregar host Realizado

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):

Nombre de dominio completo (FQDN):

Nombre de dominio completo (FQDN) para el host de destino:

☐ Eliminar este registro cuando quede obsoleto

Marca de tiempo de registro:

Período de vida (TTL): : : : (DDDDD:HH.MM.SS)

Nuevo registro de recursos [X]

Alias (CNAME)

Nombre de alias (si se deja en blanco, se usa el nombre del dominio primario):

Nombre de dominio completo (FQDN):

Nombre de dominio completo (FQDN) para el host de destino:
 [Examinar...](#)

☐ Eliminar este registro cuando quede obsoleto

Marca de tiempo de registro:

Período de vida (TTL): : : : (DDDDD:HH.MM.SS)

[Aceptar](#) [Cancelar](#)

15. You can see all the configuration.

Administrador de DNS [X]

Archivo Acción Ver Ayuda

← → ↻ ↵ ❌ 🔄 📄 ? 🖨️ 📁 📄

DNS		Nombre	Tipo	Datos
▼	WINDOWSSERVER	(igual que la carpeta princip...	Inicio de autoridad (SOA)	[1], windowsserver.daw.ne...
>	Búsquedas en caché	(igual que la carpeta princip...	Servidor de nombres (NS)	windowsserver.daw.net.
▼	Zonas de búsqueda directa			
	daw.net	windowsserver	Host (A)	192.168.1.3
		linuxclient	Host (A)	192.168.1.4
		linuxserver	Host (A)	192.168.1.2
>	Zonas de búsqueda inversa	ns	Alias (CNAME)	windowsserver.daw.net
>	Puntos de confianza	client	Alias (CNAME)	linuxclient.daw.net
>	Reenviadores condicionales	swindows	Alias (CNAME)	windowsserver.daw.net
		slinux	Alias (CNAME)	linuxserver.daw.net

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

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

Nombre: linuxclient.daw.net
Address: 192.168.1.4

C:\Windows\system32>nslookup client
Server: 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)

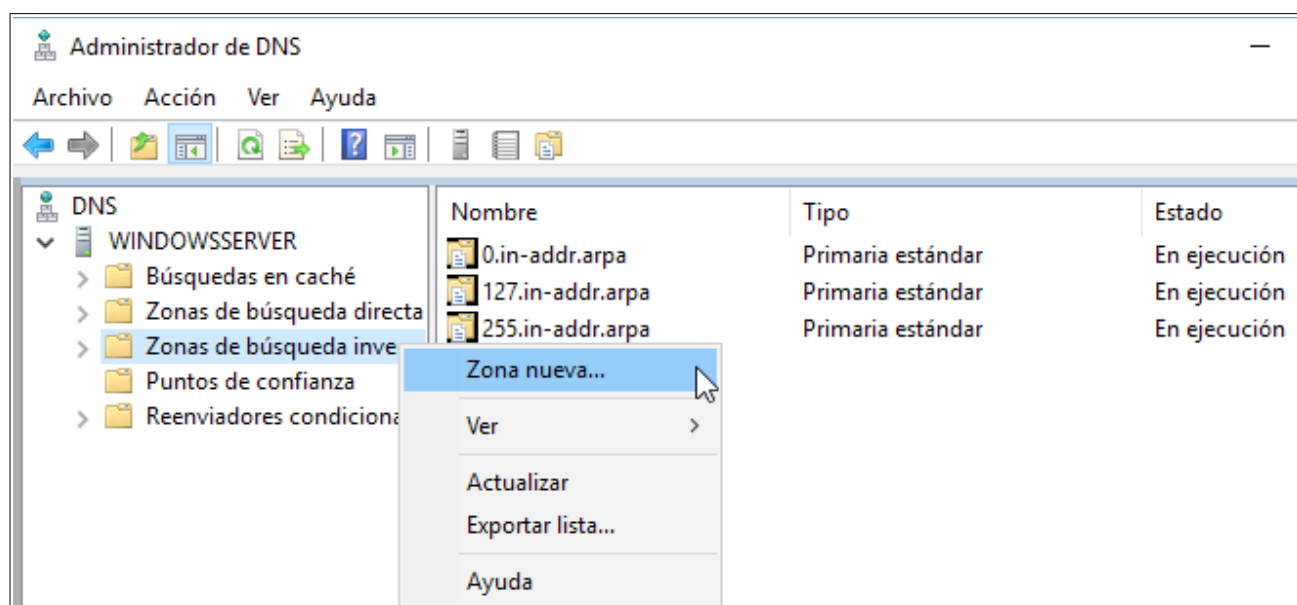
Now we are going to configure the DNS server as primary to a **reverse lookup zone**, so in this case:

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

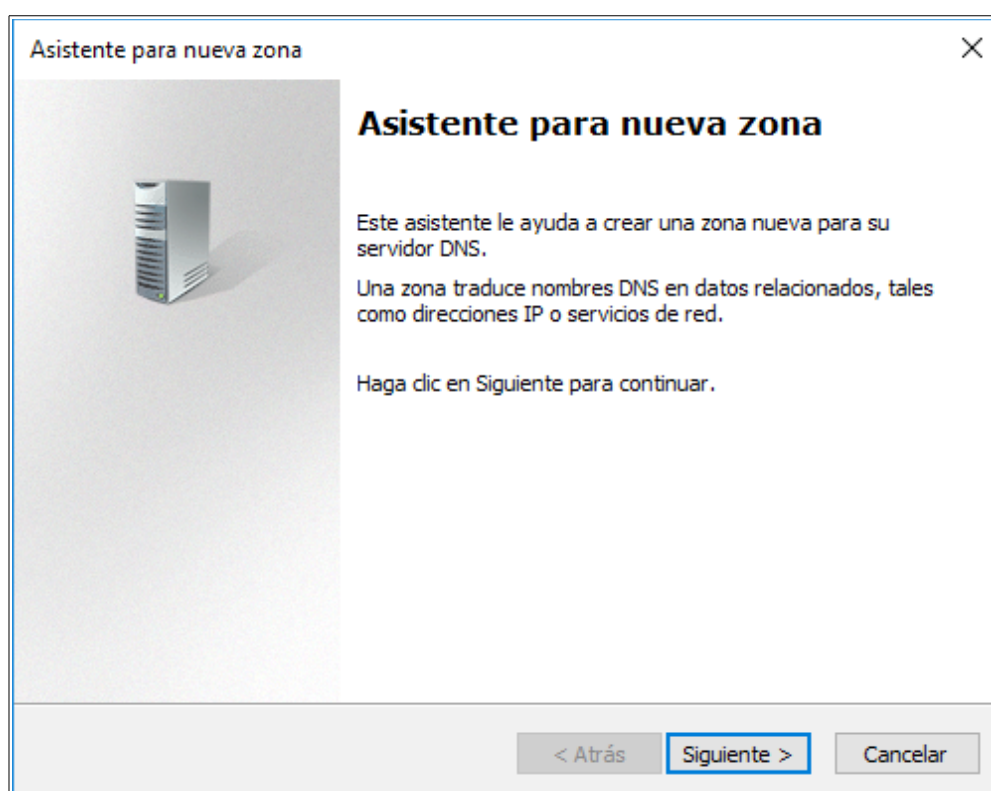
2.3.1 Configuring the reverse lookup zone

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

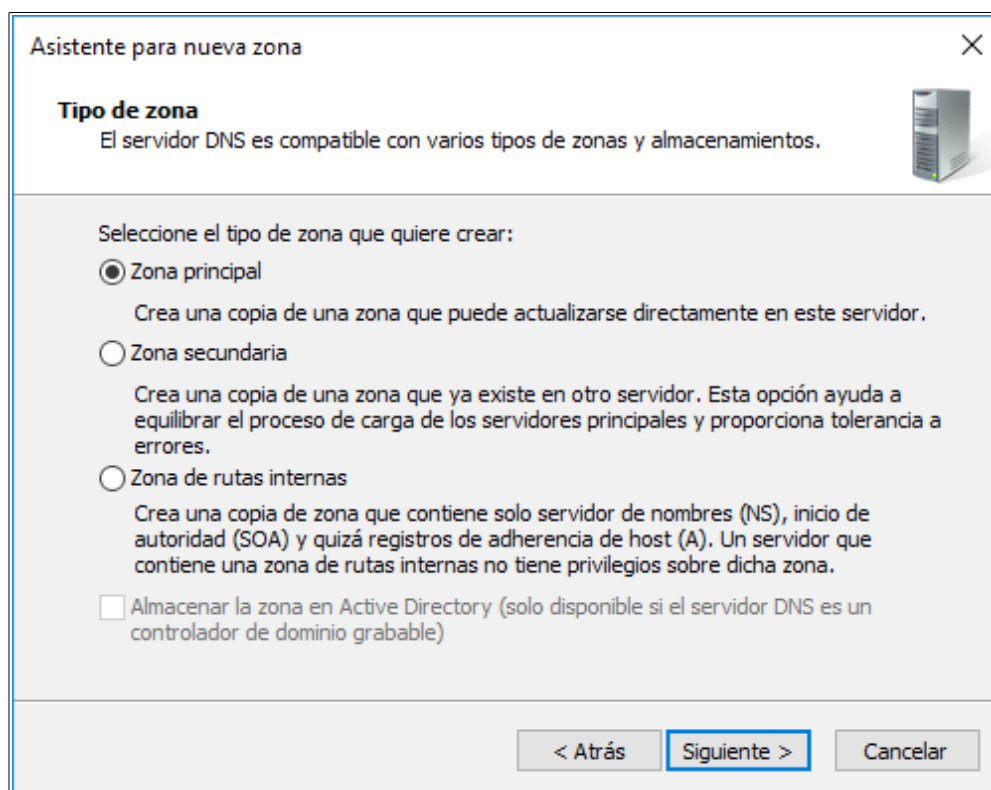
1. Go to the server administration window, click with the right button on **REVERSE LOOKUP ZONE** and click on **NEW ZONE**



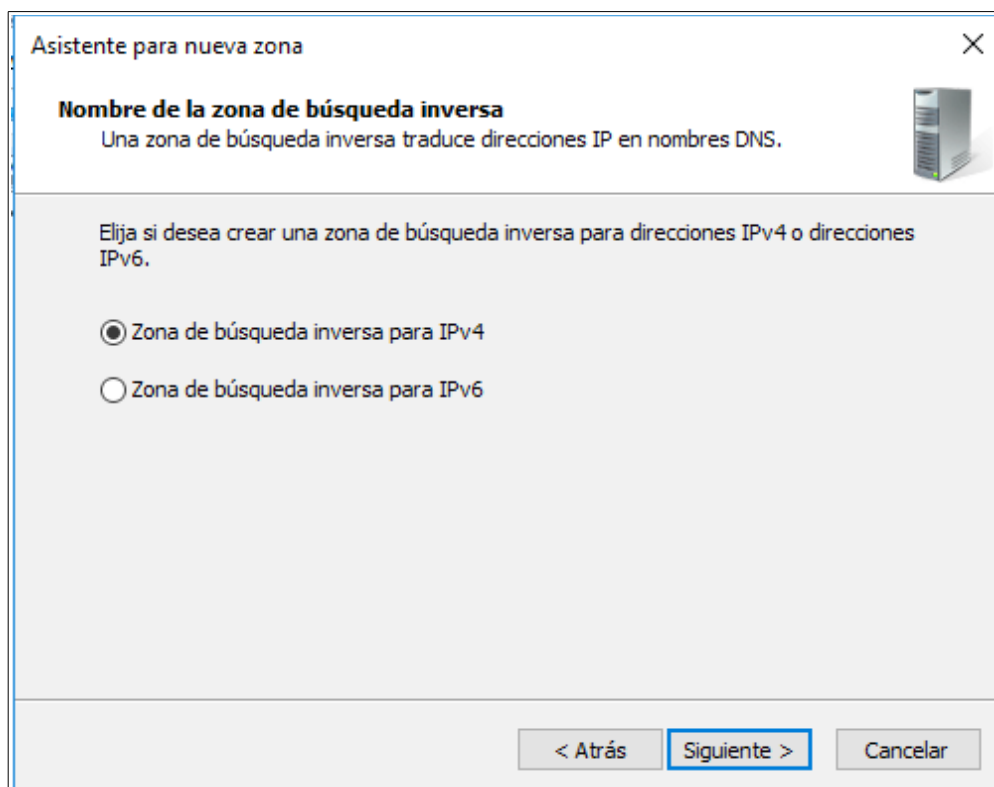
2. Read the information of the wizard and click on **NEXT**



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



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



Asistente para nueva zona

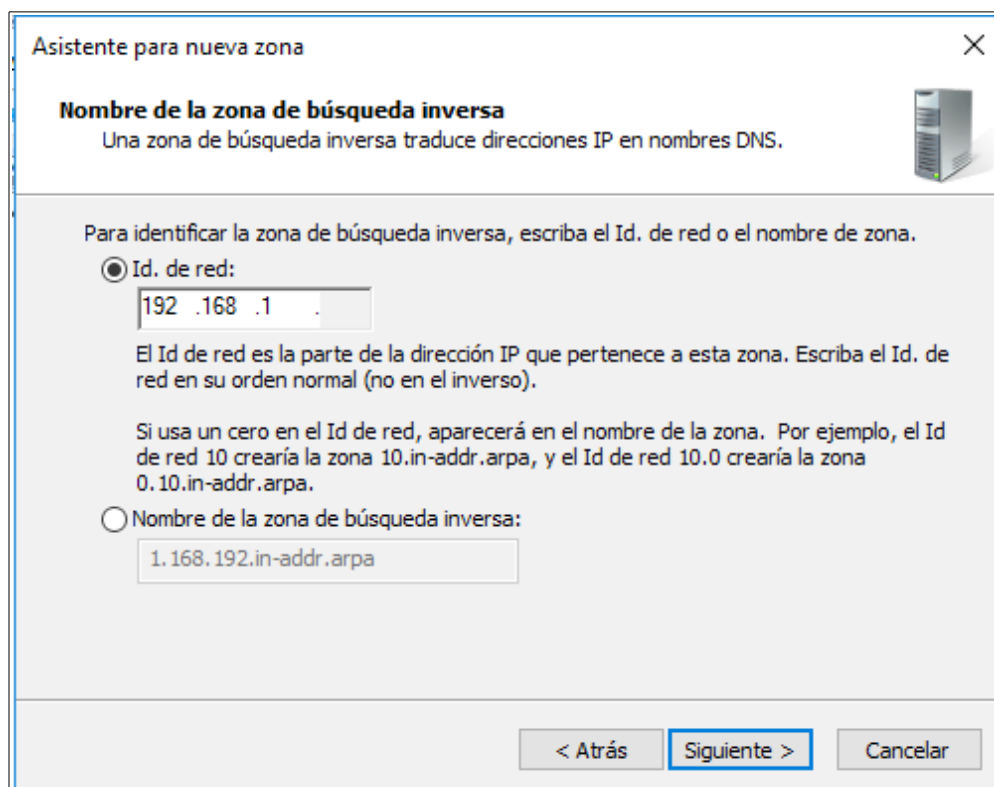
Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

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

☒ Zona de búsqueda inversa para IPv4
☐ Zona de búsqueda inversa para IPv6

< Atrás **Siguiete >** Cancelar

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



Asistente para nueva zona

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

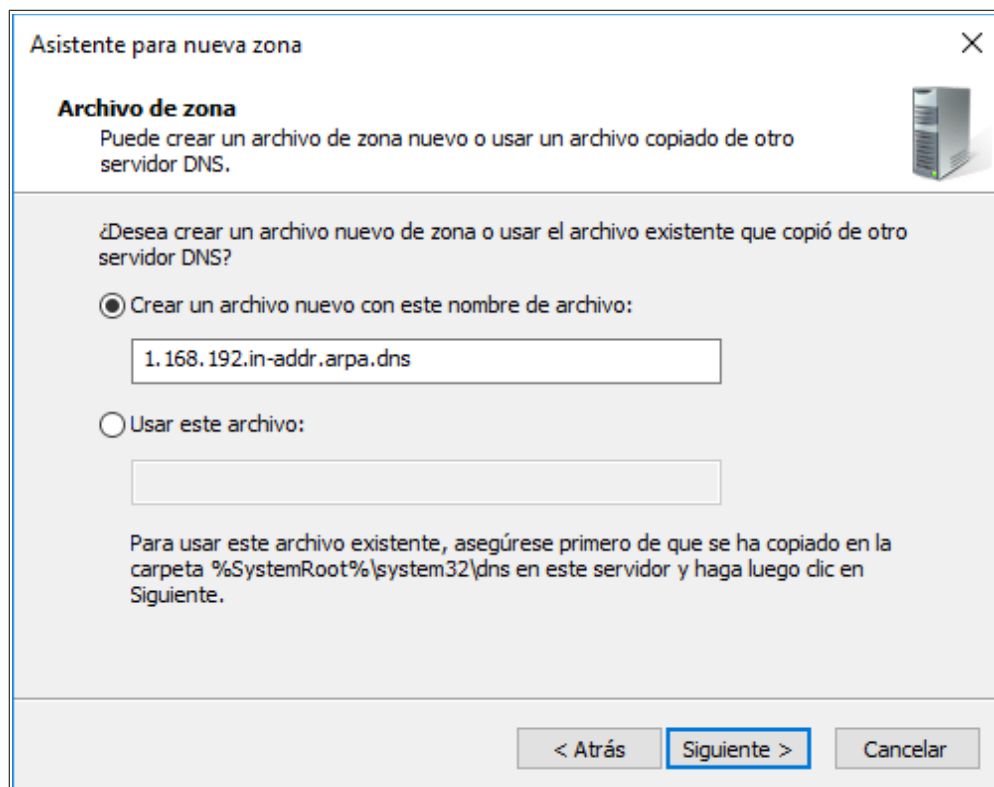
Para identificar la zona de búsqueda inversa, escriba el Id. de red o el nombre de zona.

☒ Id. de red:
192 .168 .1
El Id de red es la parte de la dirección IP que pertenece a esta zona. Escriba el Id. de red en su orden normal (no en el inverso).
Si usa un cero en el Id de red, aparecerá en el nombre de la zona. Por ejemplo, el Id de red 10 crearía la zona 10.in-addr.arpa, y el Id de red 10.0 crearía la zona 0.10.in-addr.arpa.

☐ Nombre de la zona de búsqueda inversa:
1.168.192.in-addr.arpa

< Atrás **Siguiete >** Cancelar

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




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

Asistente para nueva zona

Actualización dinámica
Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.

Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.

Seleccione el tipo de actualizaciones dinámicas que desea permitir:

- ☐ Permitir solo actualizaciones dinámicas seguras (recomendado para Active Directory)
Esta opción solo está disponible para las zonas que están integradas en Active Directory.
- ☐ Permitir todas las actualizaciones dinámicas (seguras y no seguras)
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
 Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.
- ☒ No admitir actualizaciones dinámicas
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.

< Atrás **Siguiente >** Cancelar

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

Asistente para nueva zona

Finalización del Asistente para nueva zona

Se ha completado correctamente el Asistente para nueva zona. Ha especificado la siguiente configuración:

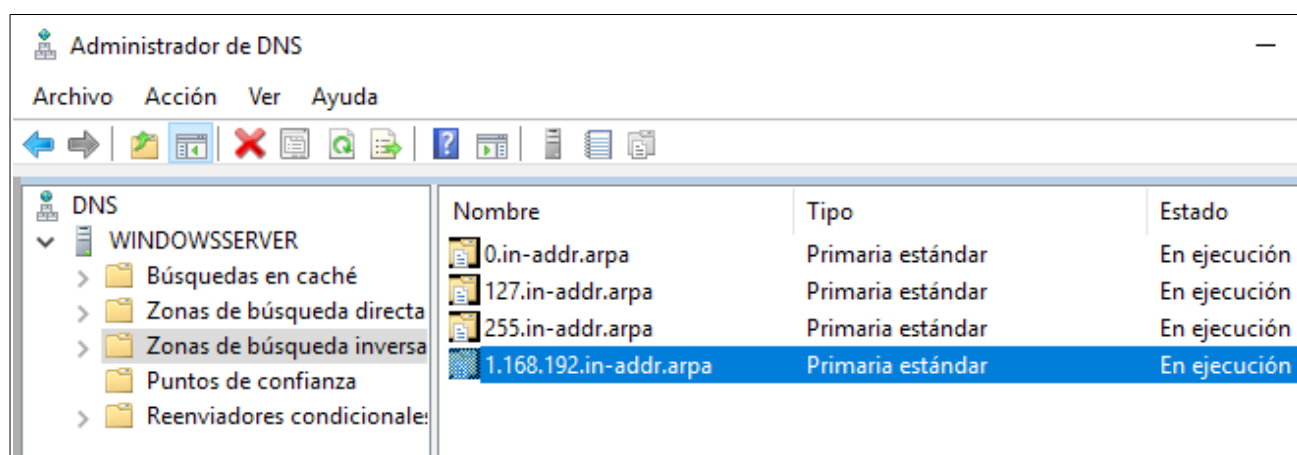
Nombre: 1.168.192.in-addr.arpa
Tipo: Primaria estándar
Tipo de búsqueda: Invertir
Nombre de archivo: 1.168.192.in-addr.arpa.dns

Nota: ahora debe agregar registros a la zona o asegurarse de que los registros se actualizan dinámicamente. A continuación, compruebe la resolución de nombres con nslookup.

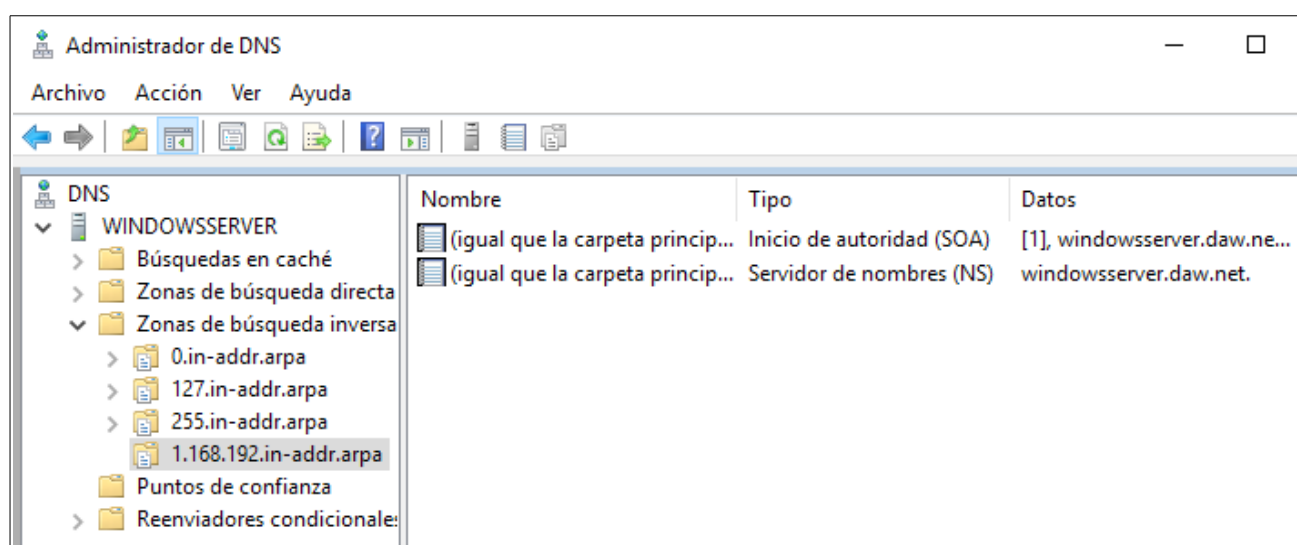
Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.

< Atrás **Finalizar** Cancelar

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.

Propiedades de 1.168.192.in-addr.arpa

Servidores de nombres WINS-R Transferencias de zona

General Inicio de autoridad (SOA)

Número de serie: 1 Incremento

Servidor principal: windowsserver.daw.net Examinar...

Persona responsable: hostmaster.daw.net Examinar...

Intervalo de actualización: 15 Minutos

Intervalo de reintento: 10 Minutos

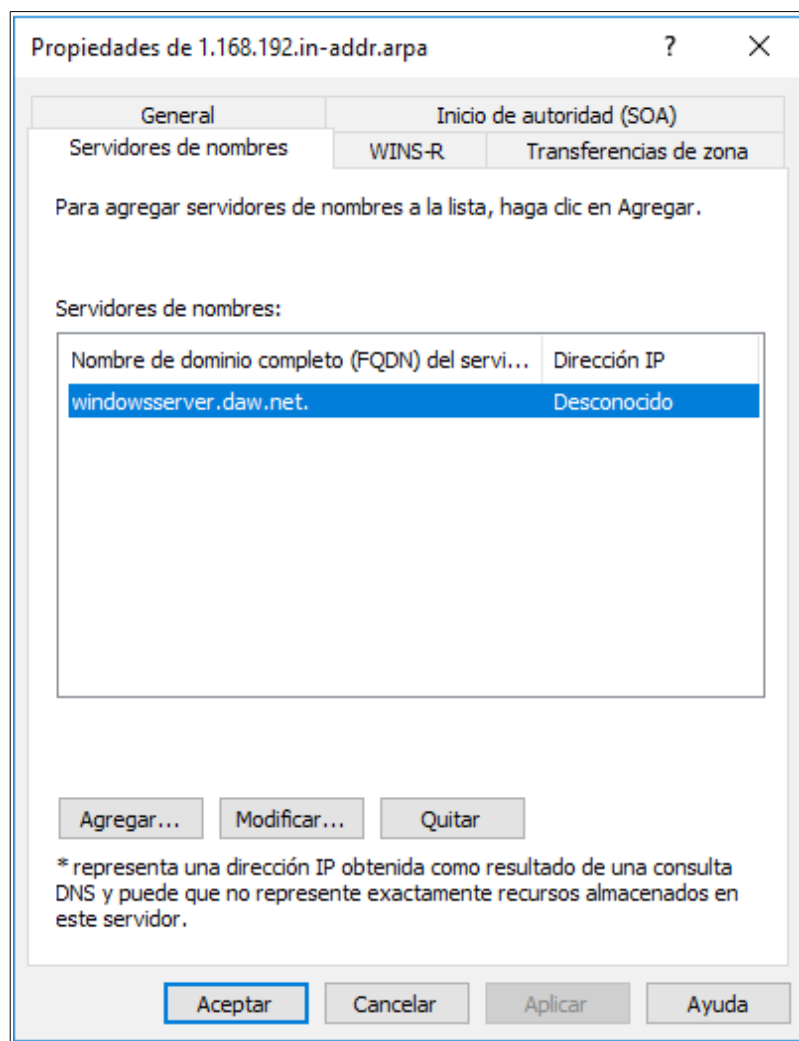
Expira después de: 1 Días

TTL mínimo (predeterminado): 1 Horas

TTL para este registro: 0 :1 :0 :0 (DDDDD:HH.MM.SS)

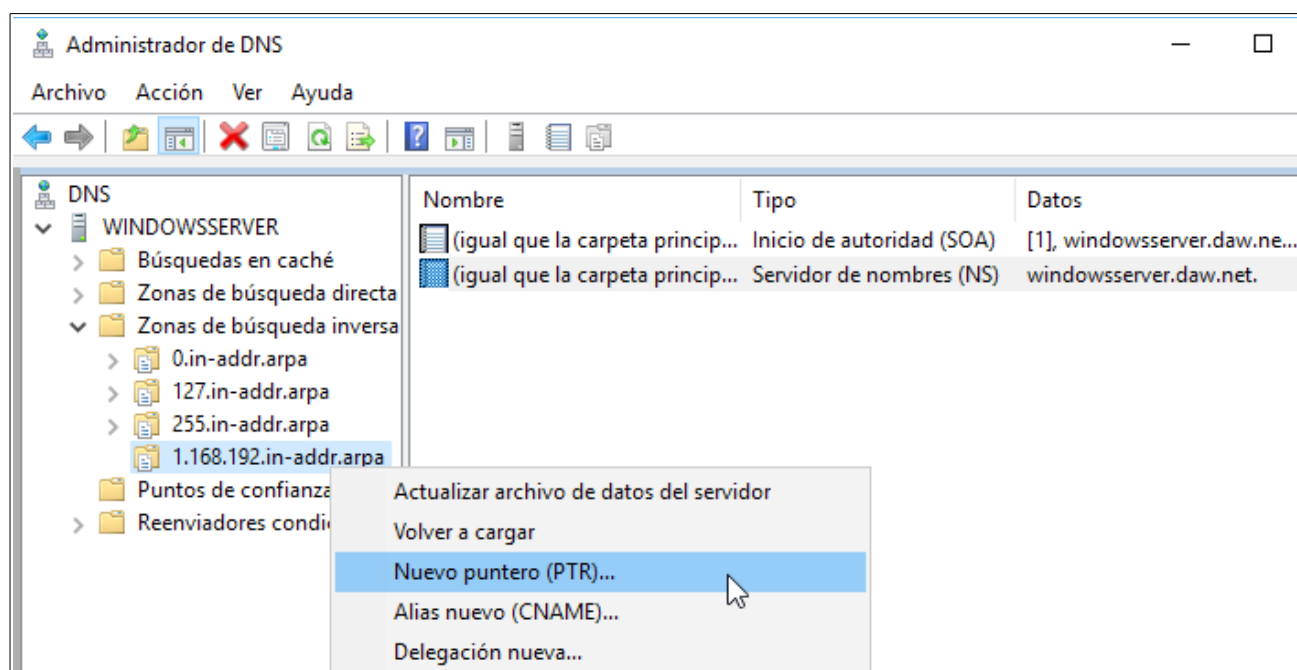
Aceptar Cancelar Aplicar Ayuda

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*



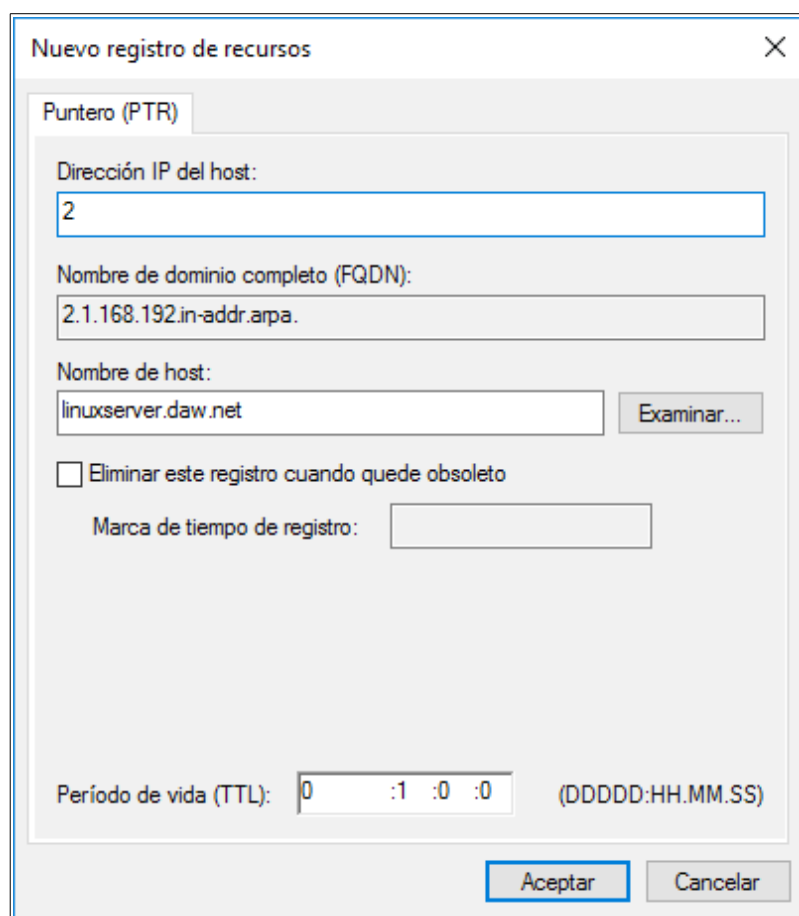
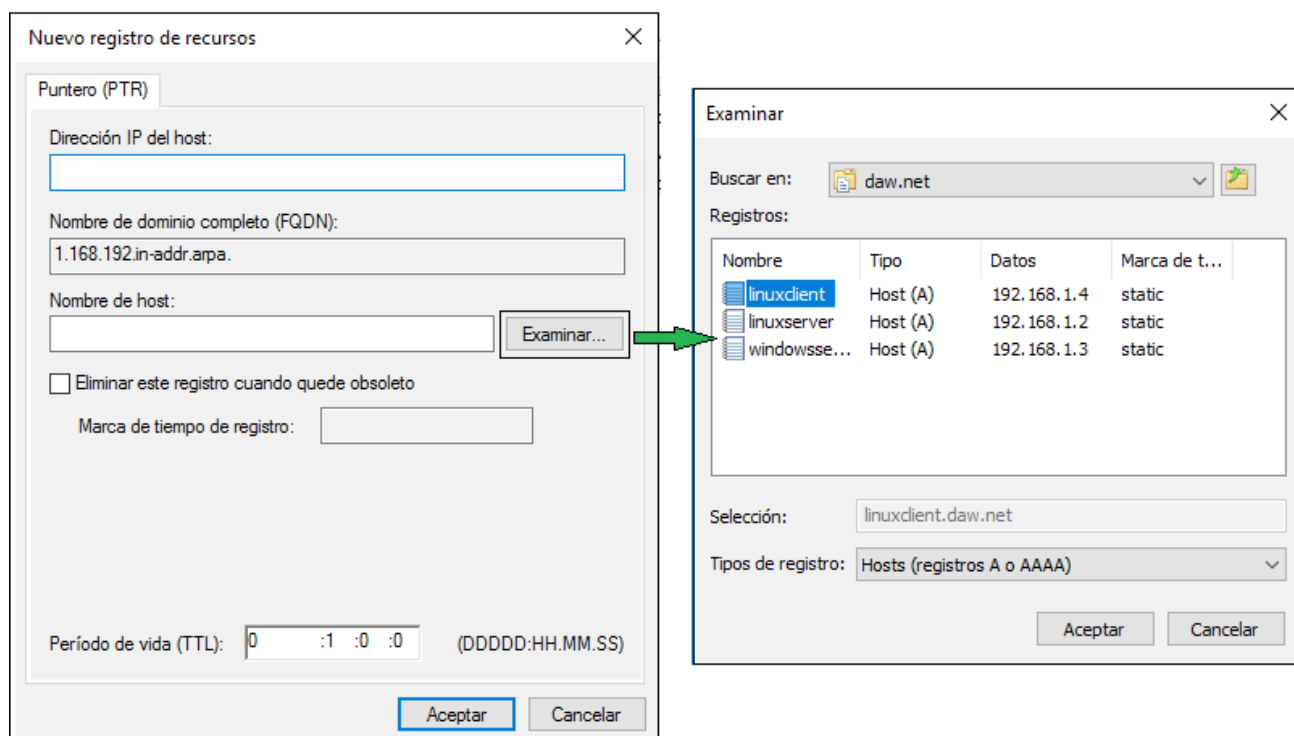
Now we are to create the **PTR** records for the names of the virtual machines

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):

Nombre de host:

☐ Eliminar este registro cuando quede obsoleto

Marca de tiempo de registro:

Período de vida (TTL): : : : (DDDDD:HH.MM.SS)

Nuevo registro de recursos [X]

Puntero (PTR)

Dirección IP del host:

4

Nombre de dominio completo (FQDN):

4.1.168.192.in-addr.arpa.

Nombre de host:

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]

14. You can see all the configuration.

Administrador de DNS

Archivo Acción Ver Ayuda

	Nombre	Tipo	Datos
DNS			
WINDOWSSERVER			
> Búsquedas en caché			
> Zonas de búsqueda directa			
> daw.net			
> Zonas de búsqueda inversa			
> 0.in-addr.arpa			
> 127.in-addr.arpa			
> 255.in-addr.arpa			
> 1.168.192.in-addr.arpa			
> Puntos de confianza			
> Reenviadores condicionales			
	(igual que la carpeta princip...	Inicio de autoridad (SOA)	[1], windowsserver.daw.ne...
	(igual que la carpeta princip...	Servidor de nombres (NS)	windowsserver.daw.net.
	192.168.1.2	Puntero (PTR)	linuxserver.daw.net
	192.168.1.3	Puntero (PTR)	windowsserver.daw.net
	192.168.1.4	Puntero (PTR)	linuxclient.daw.net

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";
};

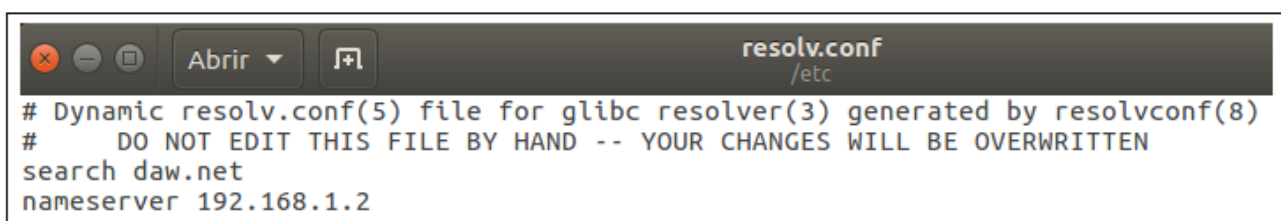
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

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:

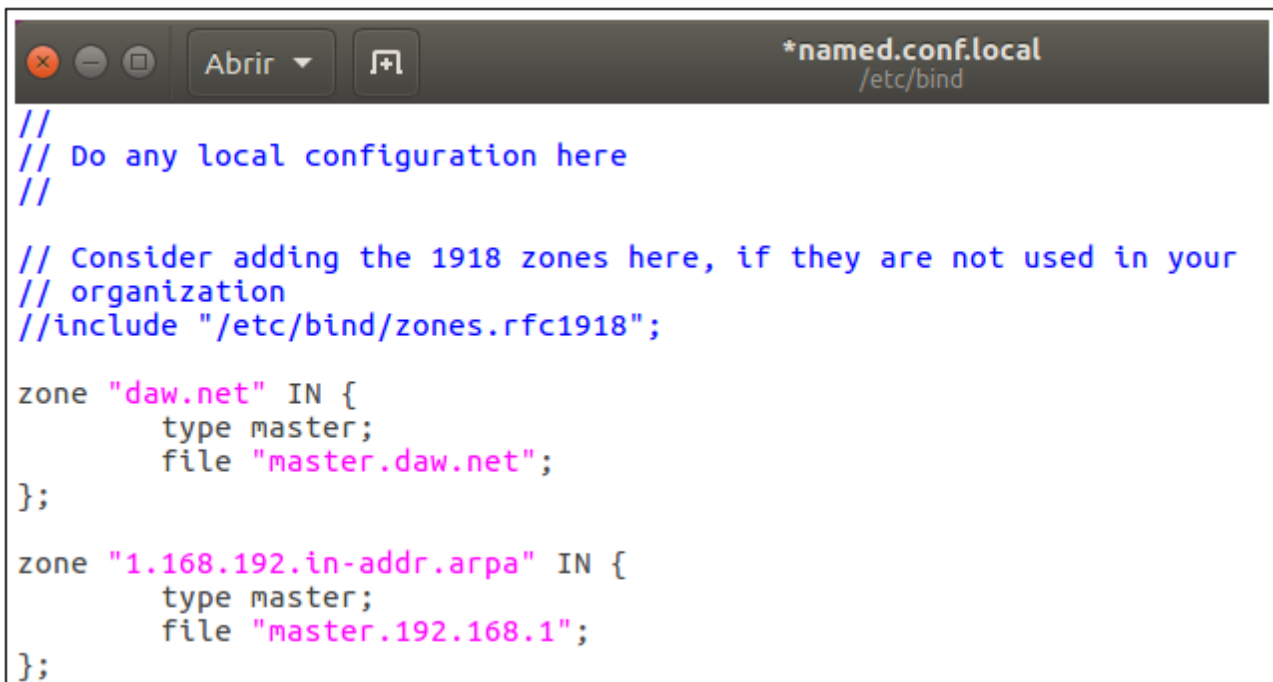


```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
search daw.net
nameserver 192.168.1.2
```

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:



```
//  
// Do any local configuration here  
//  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
zone "daw.net" IN {  
    type master;  
    file "master.daw.net";  
};  
  
zone "1.168.192.in-addr.arpa" IN {  
    type master;  
    file "master.192.168.1";  
};
```

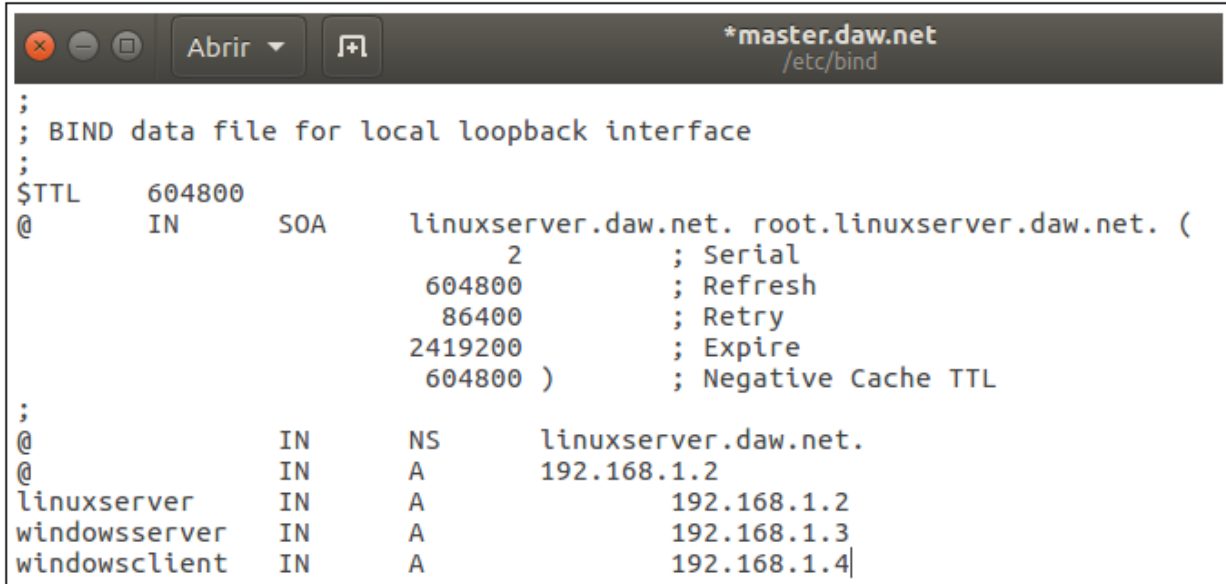
2. Now, we are going to copy the default files and create our master files:

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**.

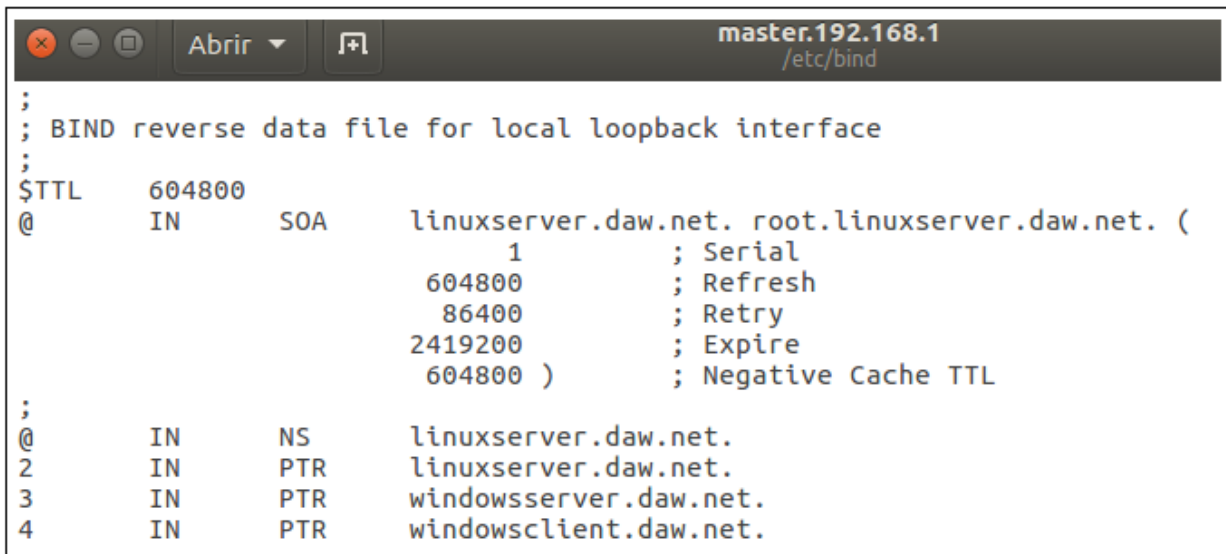


```

;
; 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).



```

;
; 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/cache/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
```

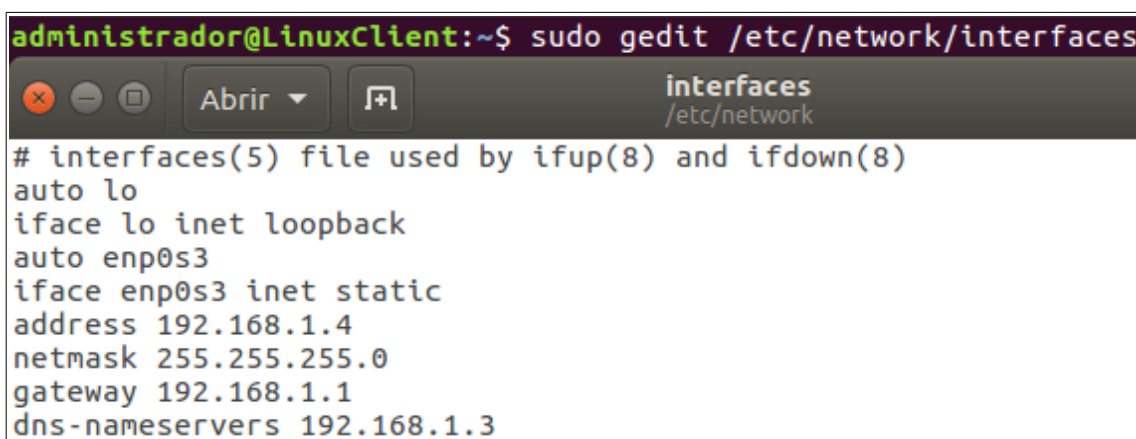
```
administrador@LinuxServer:/etc/bind$ nslookup 192.168.1.3
Server:      192.168.1.2
Address:     192.168.1.2#53

3.1.168.192.in-addr.arpa      name = windowserver.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
```



```
# 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.conf
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.

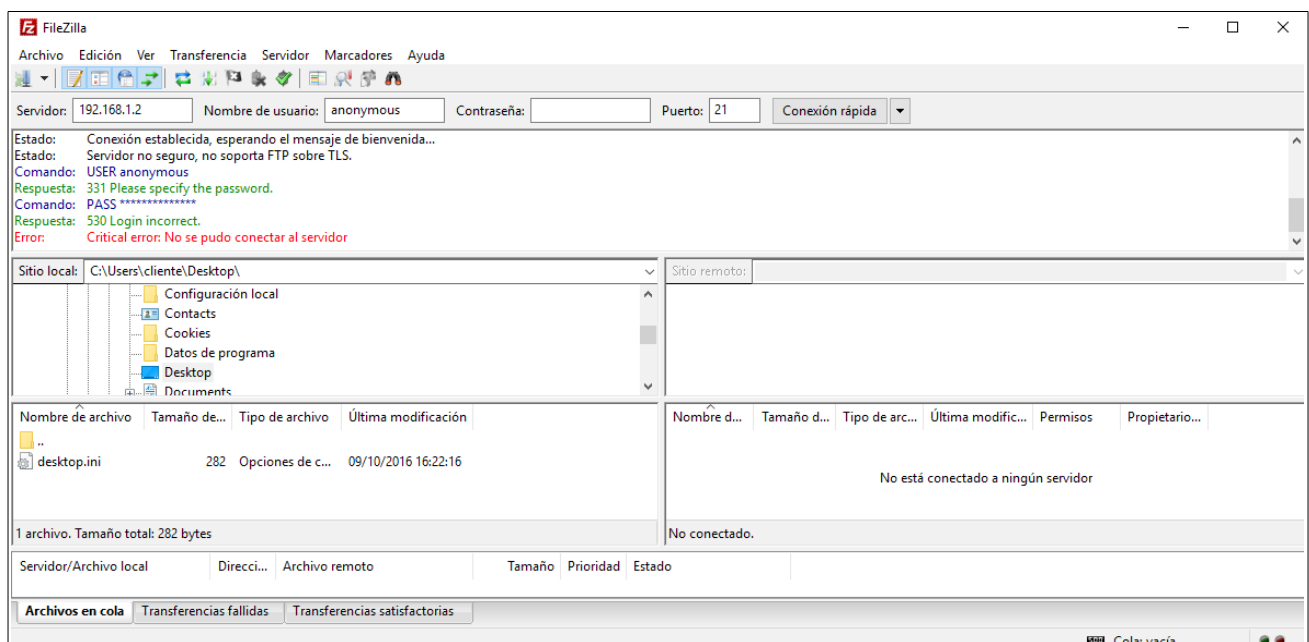
- **local_enable=YES** it is enabled the access to the local users.
- **#write_enable=YES** it is commented the directive to allow upload files to the server. So it is forbidden.

Now we are going to test the connection from **linuxclient** or **windowserver** 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.

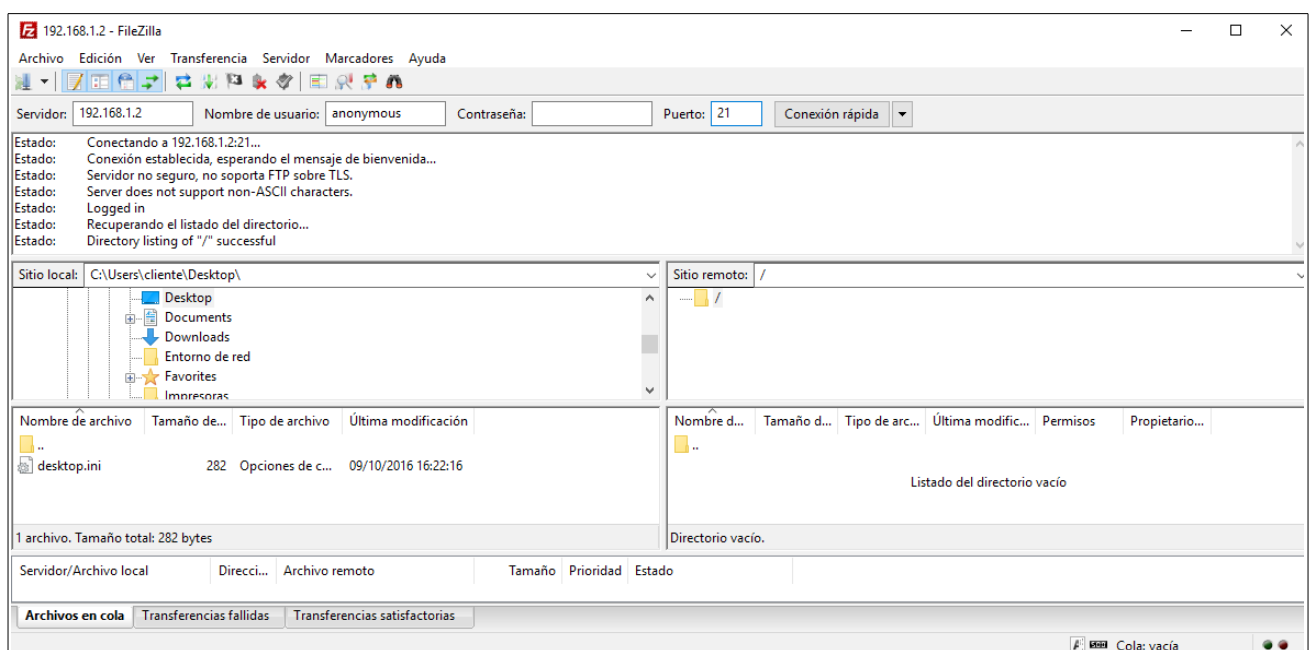
Now, we are going to enable the access to anonymous. We are going to edit the configuration file and change **anonymous_enable=NO** to **anonymous_enable=YES**

```

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

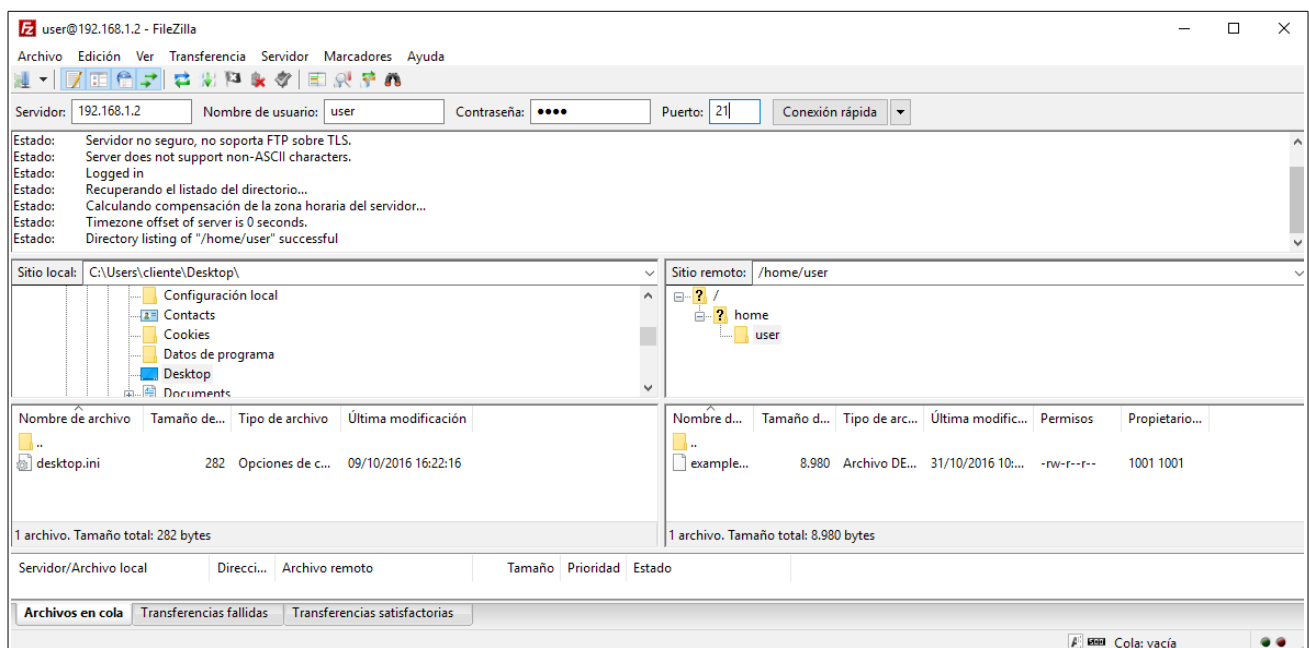


Now we can connect to the server but we can not to transfer files because we are anonymous. So,

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
Cambiano 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
```

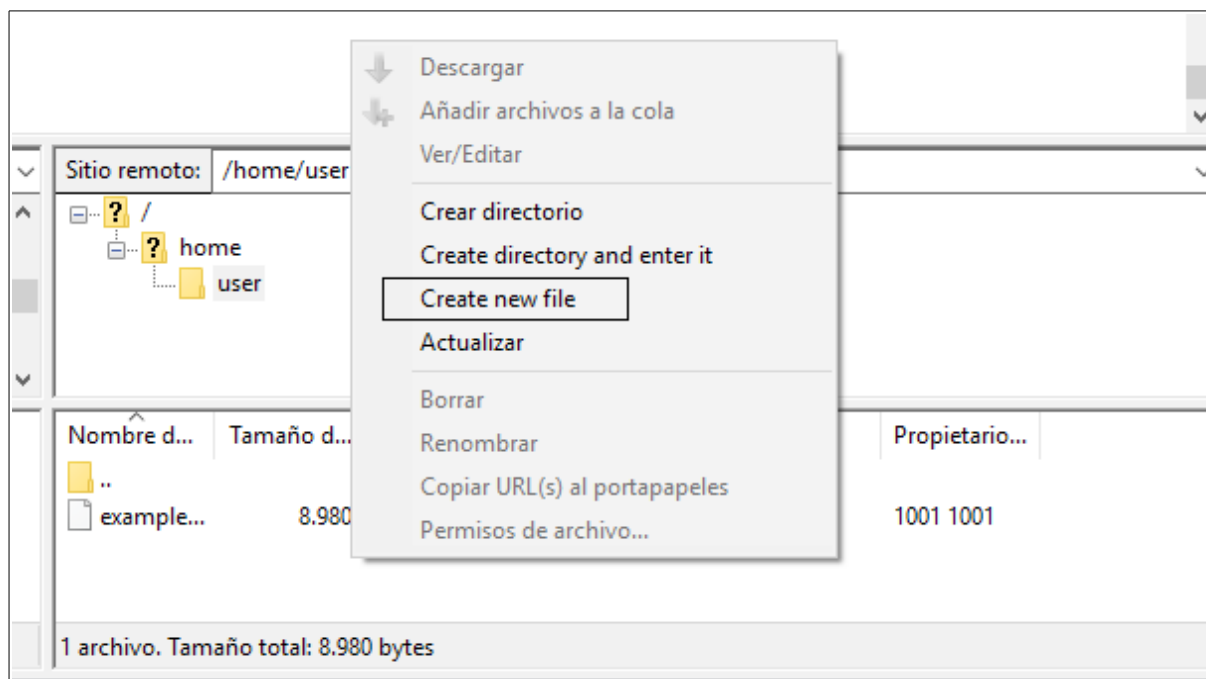
And connect using that user:

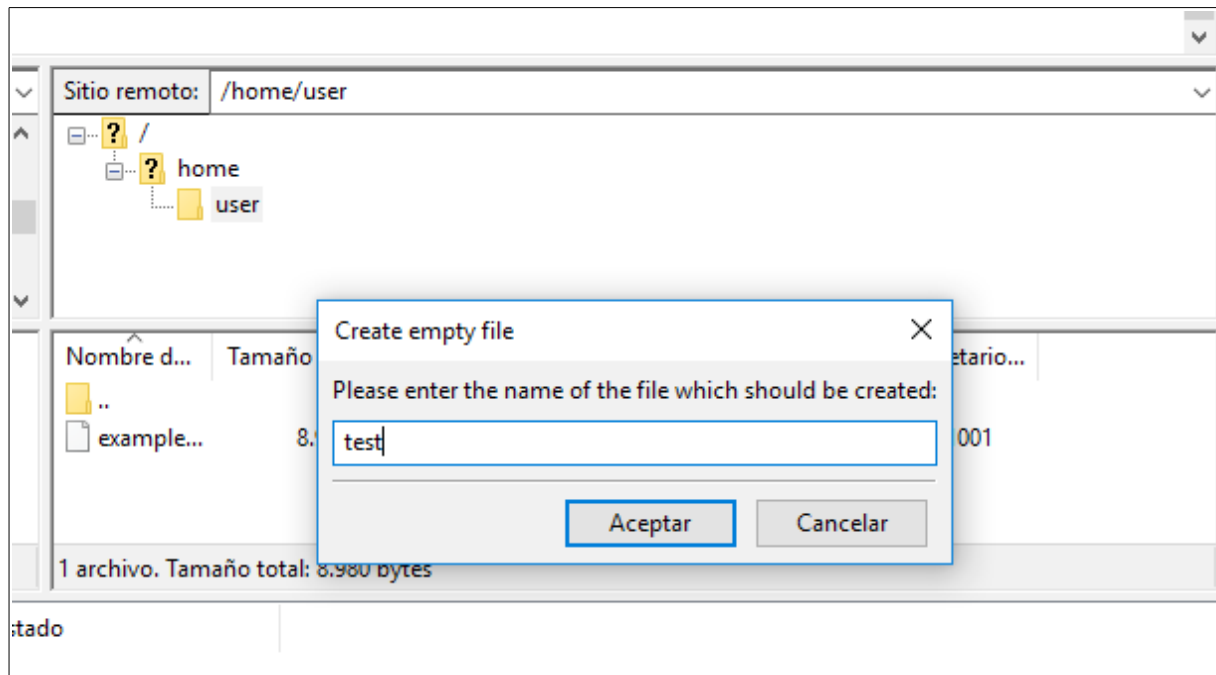


Now we can access but we can not transfer or create any file because of the directive *#write_enable=YES*, so we are going to uncomment it:

```
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):





Sitio local: C:\Users\cliente\Desktop\				Sitio remoto: /home/user			
<ul style="list-style-type: none"> Datos de programa Desktop Documents Downloads Entorno de red Favorites 				<ul style="list-style-type: none"> home user 			
Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación	Nombre d...	Tamaño d...	Tipo de arc...	Última modifi...
..				..			
desktop.ini	282	Opciones de c...	09/10/2016 16:22:16	example...	8.980	Archivo DE...	31/10/2016 10:...
test	0	Archivo	31/10/2016 9:57:14	test	0	Archivo	31/10/2016 10:...
2 archivos. Tamaño total: 282 bytes				2 archivos. Tamaño total: 8.980 bytes			

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`

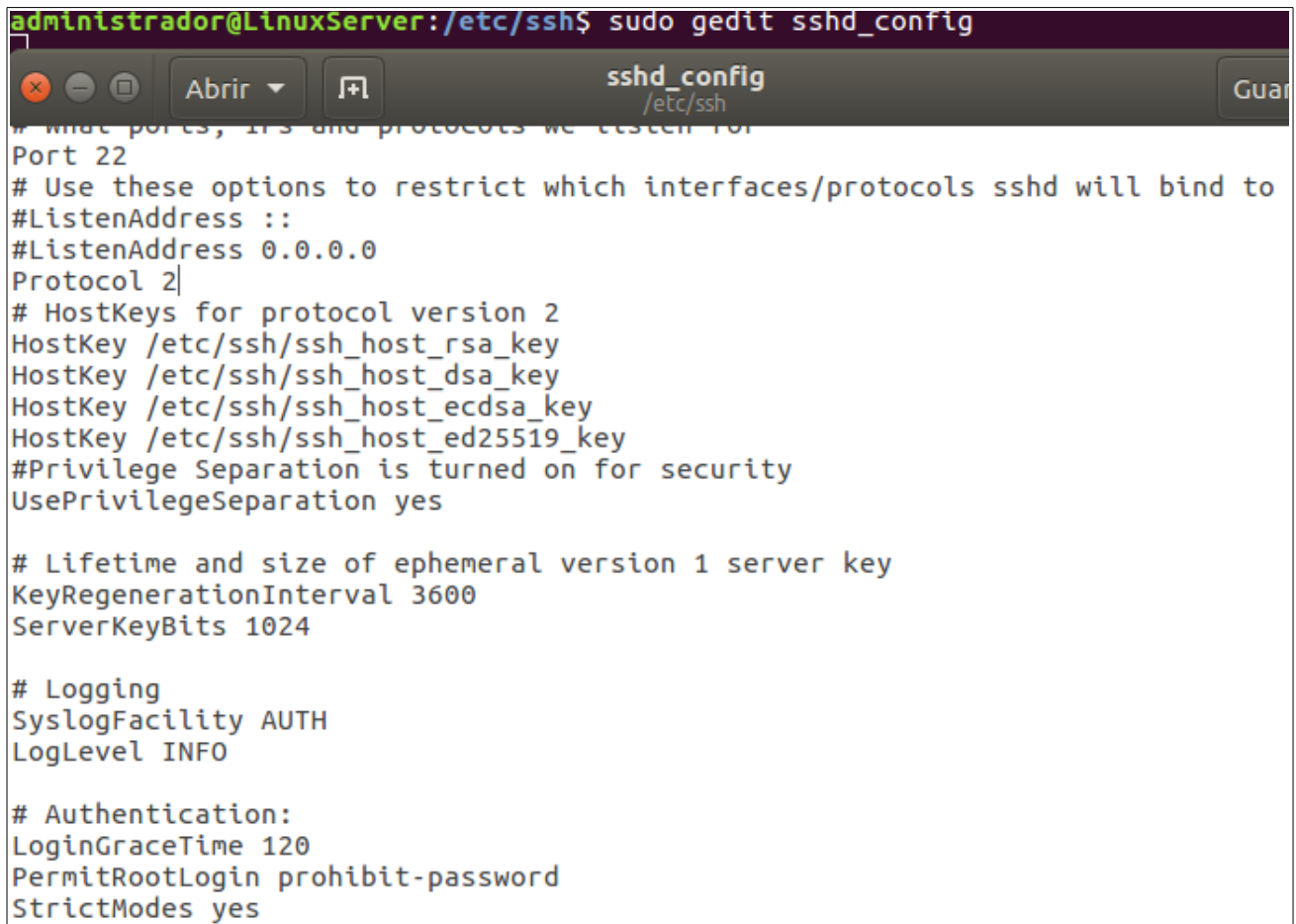
```
administrador@LinuxServer:~$ ps -ef | grep ssh
root      18465      1  0 10:01 ?        00:00:00 /usr/sbin/sshd -D
adminis+  18540    2326  0 10:03 pts/4    00:00:00 grep --color=auto ssh
administrador@LinuxServer:~$ netstat -ltn
Conexiones activas de Internet (solo servidores)
Proto Recib Enviad 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`:



```
adminstrador@LinuxServer:/etc/ssh$ sudo gedit sshd_config
# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin prohibit-password
StrictModes yes
```

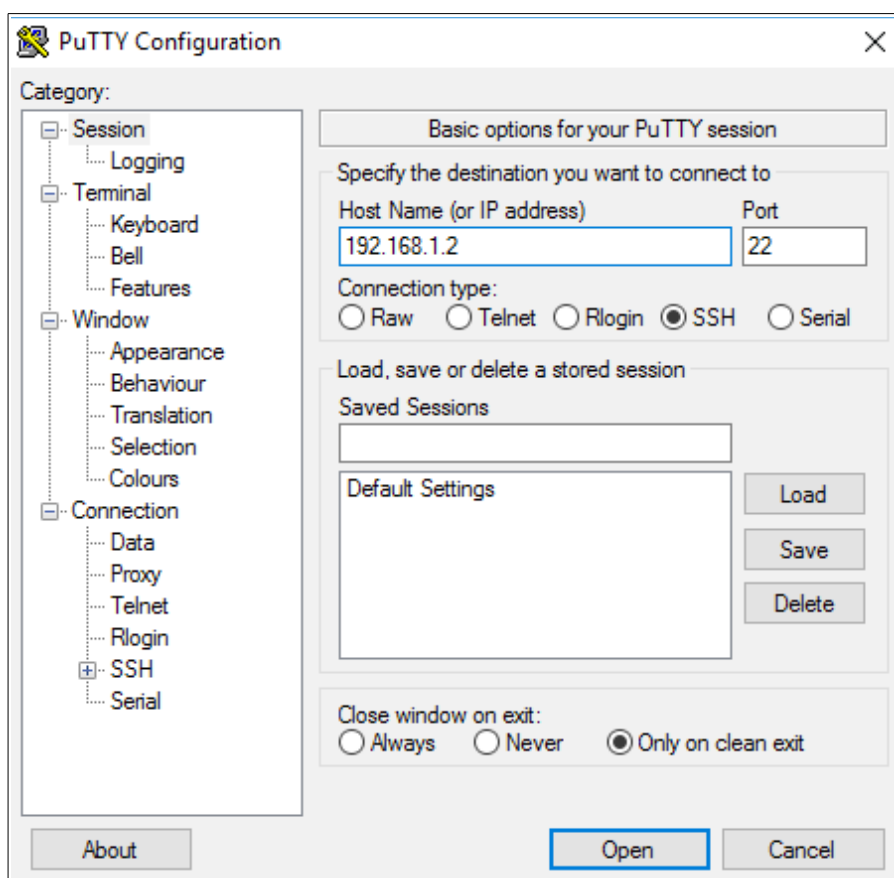
We can take a look to the listening port 22, the different private keys or the forbidden access to the root (**PermitRootLogin prohibit-password**).

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:

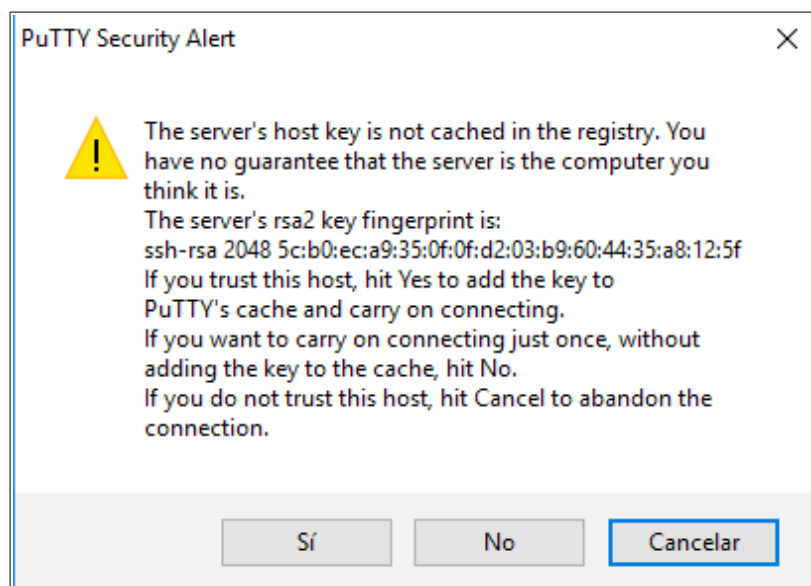
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

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:

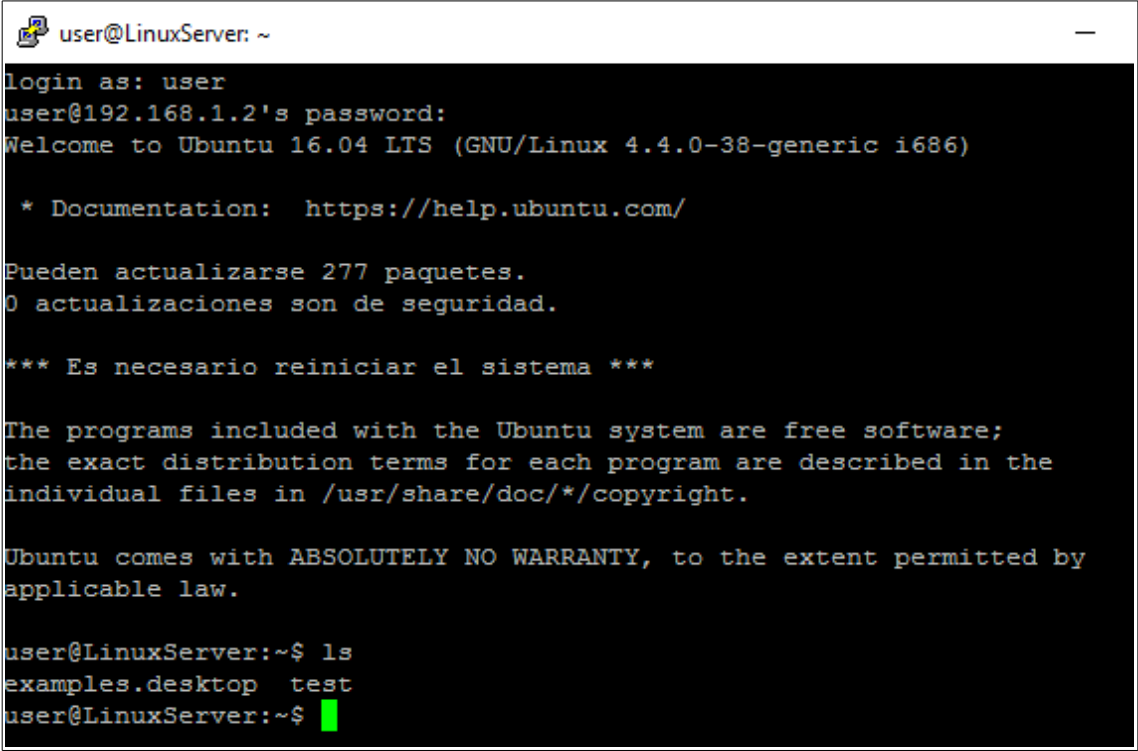


Now, we are going to check if that fingerprint is the same as our server. For that we write in the terminal: **ssh-keygen -l -E MD5 -f /etc/ssh/ssh_host_rsa_key.pub**

```
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**:

A terminal window titled 'user@LinuxServer: ~' with a standard Ubuntu logo icon. The terminal output shows a login process for 'user' at IP '192.168.1.2'. It displays the Ubuntu 16.04 LTS welcome message, documentation link, and system update information (277 packages, 0 security updates). It also shows the standard Ubuntu disclaimer about free software and warranty. Finally, the user runs the 'ls' command, showing 'examples.desktop' and 'test' files in the home directory.

```
user@LinuxServer: ~  
login as: user  
user@192.168.1.2's password:  
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-38-generic i686)  
  
 * Documentation:  https://help.ubuntu.com/  
  
Pueden actualizarse 277 paquetes.  
0 actualizaciones son de seguridad.  
  
*** Es necesario reiniciar el sistema ***  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
user@LinuxServer:~$ ls  
examples.desktop  test  
user@LinuxServer:~$
```