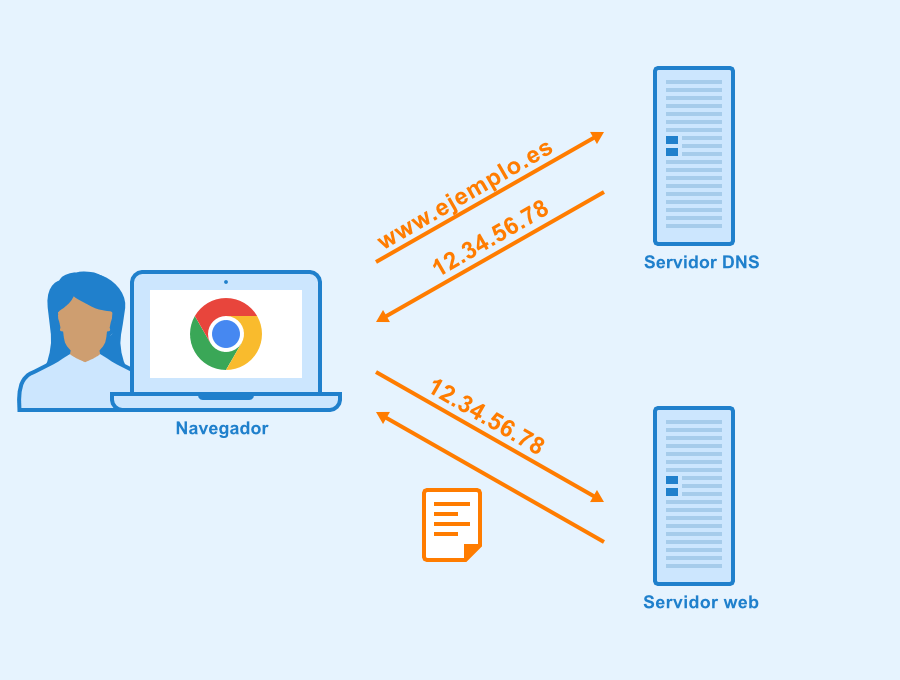
**Dibujo de una persona

Descripción generada automáticamente con confianza baja**

***SERVIDOR DNS***





**Achraf El mahjouby Sourour**

ÍNDICE

Contenido

[***Introducción*** 3](#_Toc183021330)

[***Creación del DNS en Windows*** 3](#_Toc183021331)

[***Creación de Zonas Windows*** 8](#_Toc183021332)

[***Comprobaciones de zonas directas e inversas*** 18](#_Toc183021333)

[***Servidor DNS en Linux*** 20](#_Toc183021334)

[***Agregar zonas*** 25](#_Toc183021335)

[***Configuración de zonas*** 26](#_Toc183021336)

[***Comprobación de zonas*** 31](#_Toc183021337)

[***Conclusión*** 32](#_Toc183021338)

[**Servidor DNS en Linux (Bind9):** 32](#_Toc183021339)

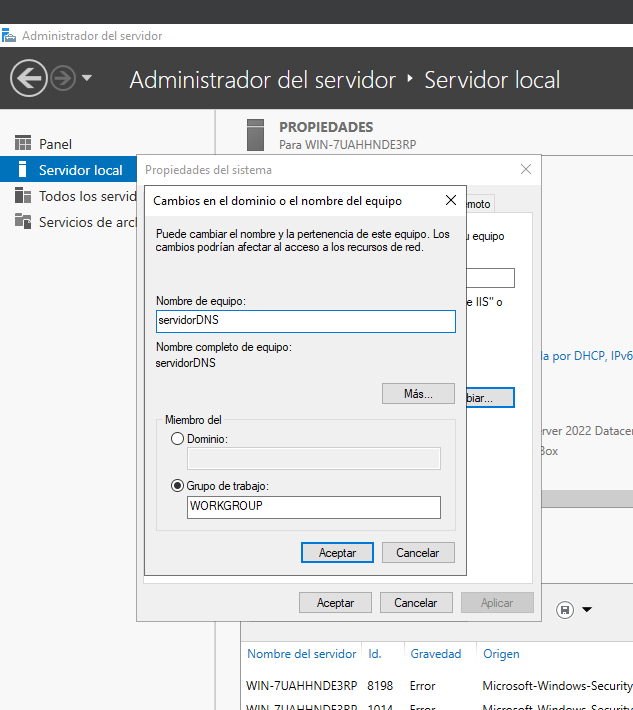
[**Servidor DNS en Windows (DNS Server):** 32](#_Toc183021340)

# ***Introducción***

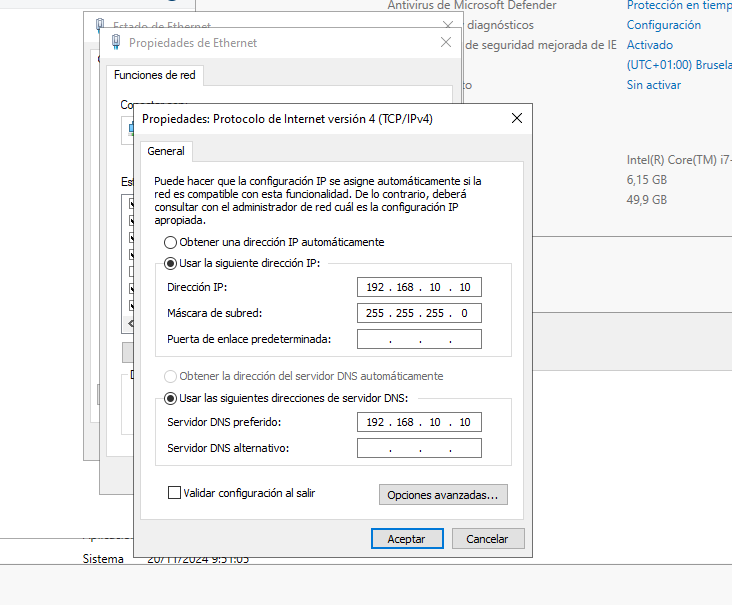
En la siguiente practica crearemos una maquina servidora en nuestro caso con Windows 2022 y con Linux Ubuntu en la que instalaremos el rol de DNS y agregaremos zonas de búsqueda directa/inversa y realizaremos comprobaciones, tanto en Linux como en Windows

# ***Creación del DNS en Windows***

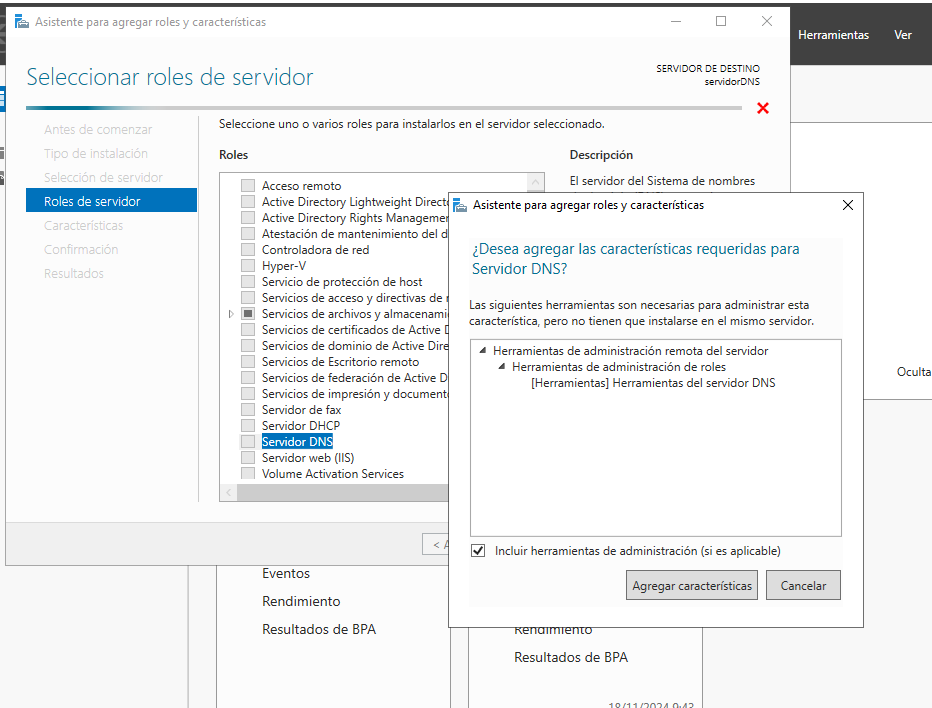
Lo primero que hemos hecho después crear la maquina es cambiarle el nombre a servidorDNS como se puede observar en la siguiente imagen.



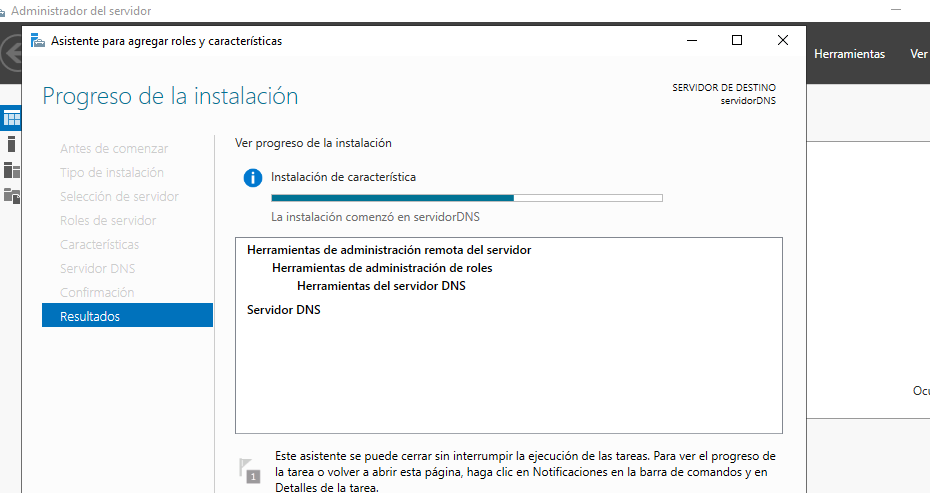
Lo siguiente que hacemos es asignarle una IP estática y ponerla en red interna en nuestro caso le hemos puesto la 192.168.10.10 y la loopback o si misma en el DNS preferido que es la 127.0.0.1 o la 192.168.10.10 .



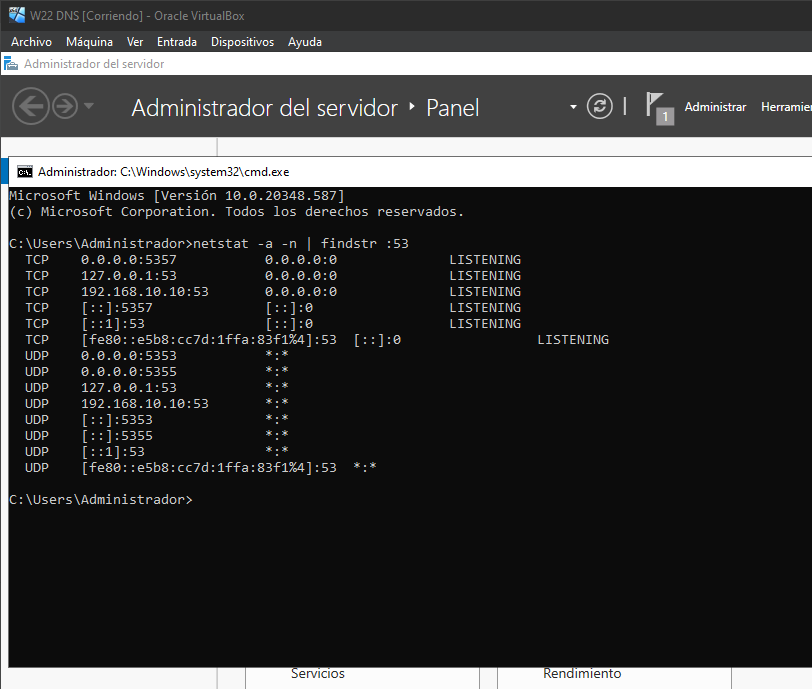
Una vez asignada la IP podemos empezar tenemos que agregarle el rol de servidor DNS para ello lo instalamos.



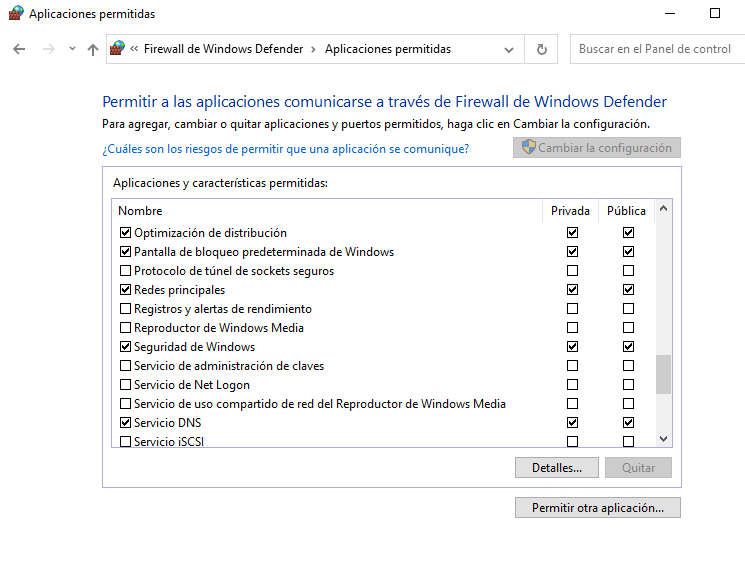
Y como podemos comprobar se finalizó la instalación de manera exitosa



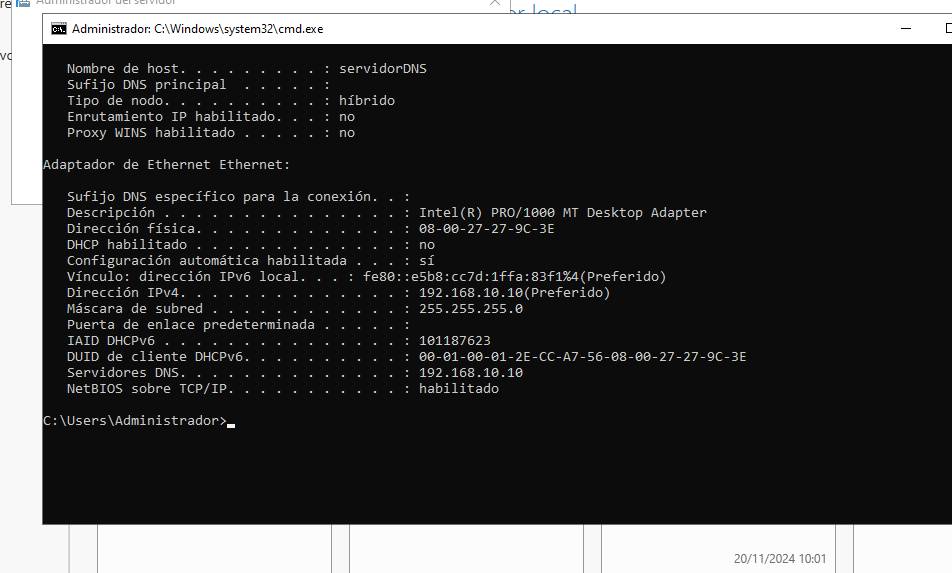
Para comprobar si lo hemos instalado bien tenemos que poner este comando “netstat -a -n | findstr :53” hemos puesto el :53 ya que le servidor DNS escucha por el puerto 537TCP y 53/UDP.



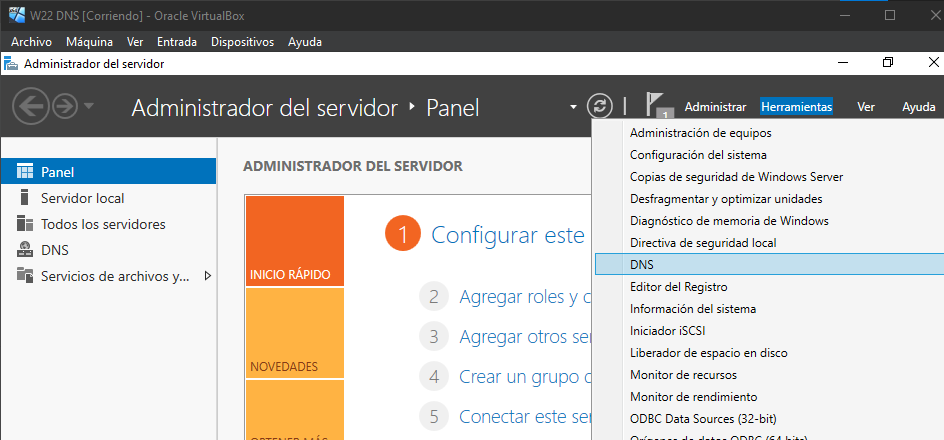
También tenemos que comprobar si el Firewall no deja comunicarnos con el exterior para ello tenemos que habilitarlo desde el panel de control.



Lo siguiente que podemos hacer para comprobar la IP del servidor DNS, abrimos un CMD y ejecutamos el IPconfig /all y cómo podemos comprobar nos da la IP de ella misma es decir la loopback.



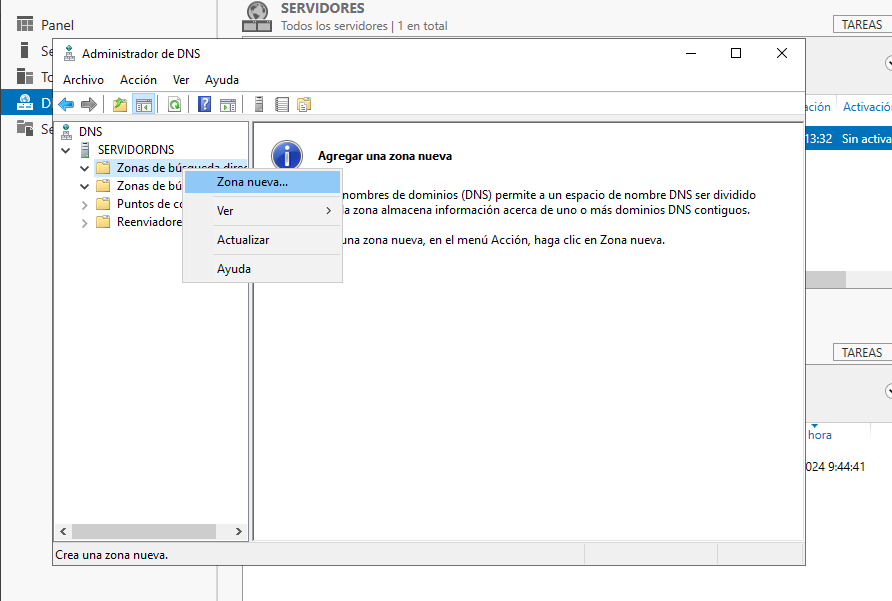
Una vez instalado y configuradas sus IPs pasamos a configurar las zonas para ellos dentro del servidor nos dirigimos a la herramienta del DNS.



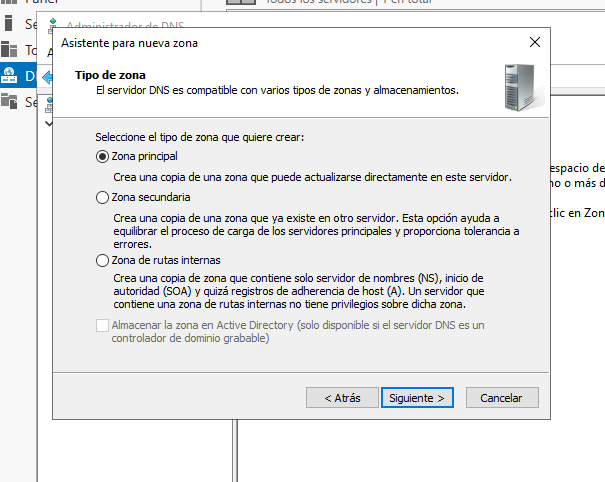
## ***Creación de Zonas Windows***

Nos abre una ventana en la que aparece nuestro servidor DNS y dentro de el las zonas tanto la directa como la inversa

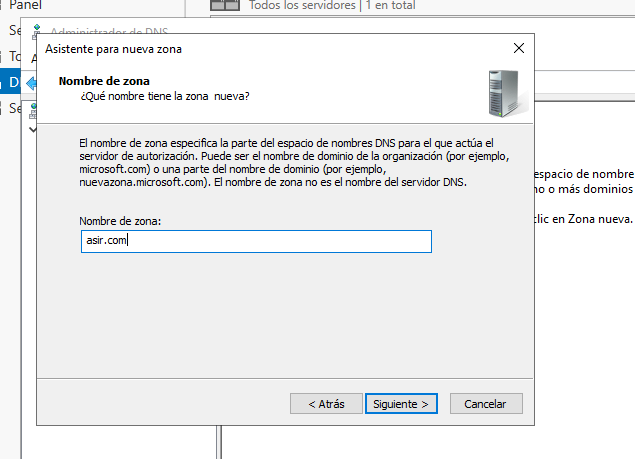
En nuestro caso crearemos una nueva zona directa



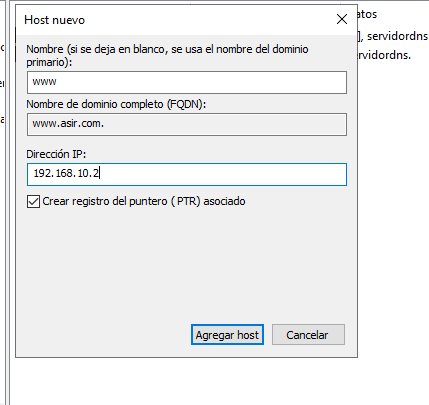
Cómo es la primera que hacemos, la dejamos como zona principal.



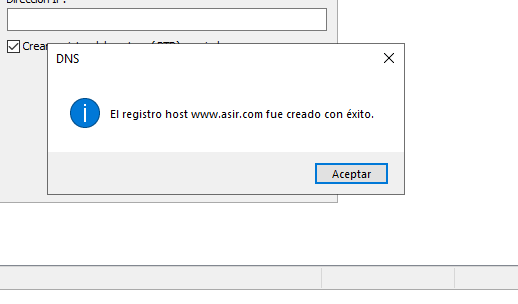
El siguiente paso es asignarle un nombre a la zona en mi caso he puesto “asir.com” aunque luego creemos otra distinta.



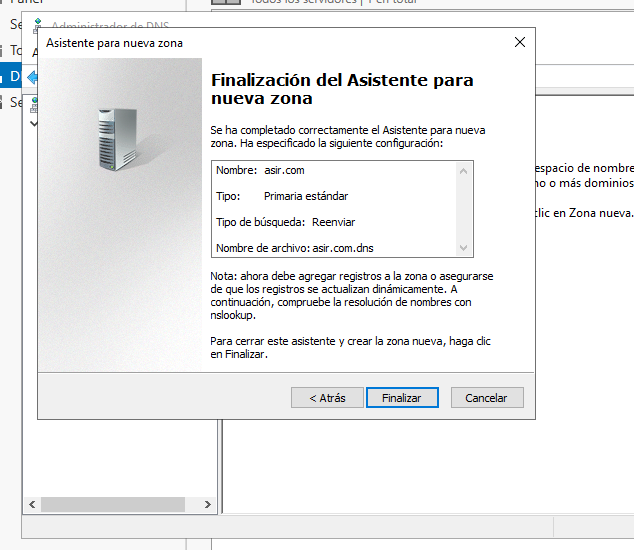
Una vez asignado el nombre tenemos que crear un nuevo host , le he llamado www.asir.com y le asignamos una IP en mi caso le he puesto la 192.168.10.2.



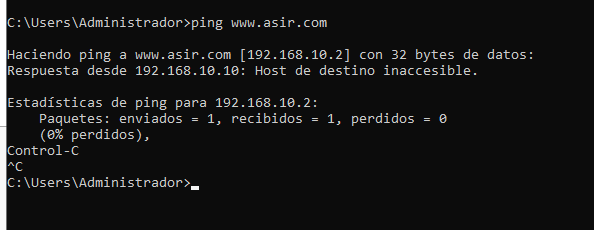
Y se puede observar que se ha agregado correctamente



Y ya la finalizaríamos correctamente

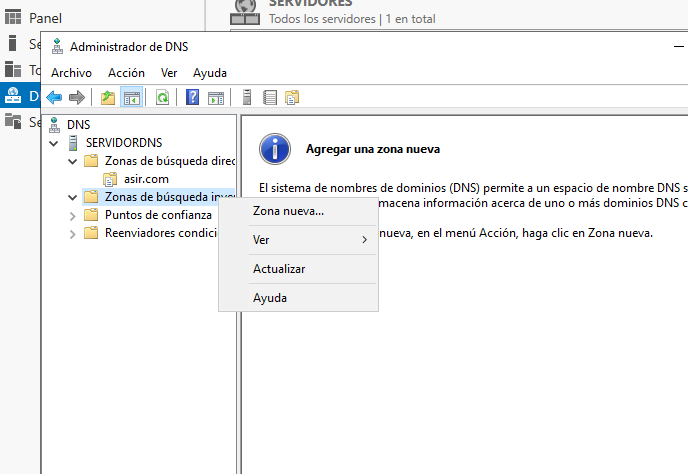


Para comprobar si la zona directa se ha creado correctamente, abrimos un CMD y hacemos un ping al nombre del host y esperamos a que nos devuelva la IP asignada anteriormente.

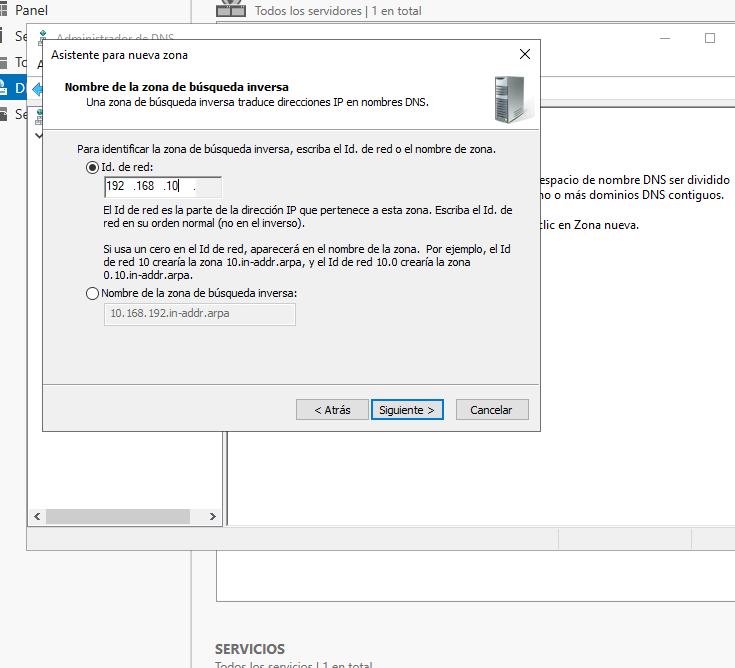


Lo siguiente que tenemos que hacer es lo contrario asignar un nombre es decir crear una zona inversa para que cada vez que se busquemos una IP nos de el nombre del host

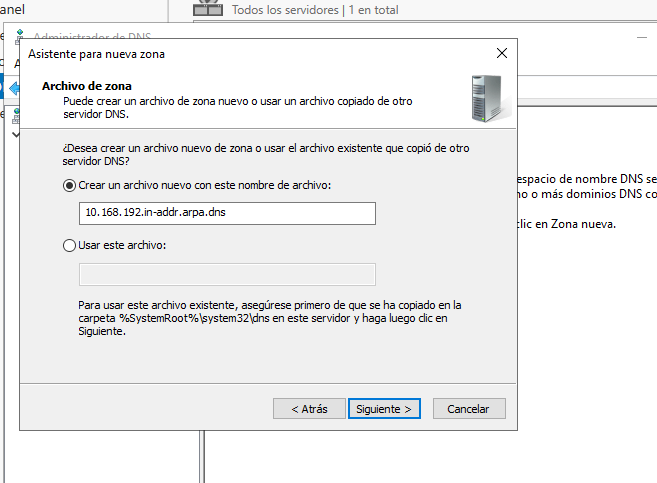
Para ello creamos una nueva zona inversa



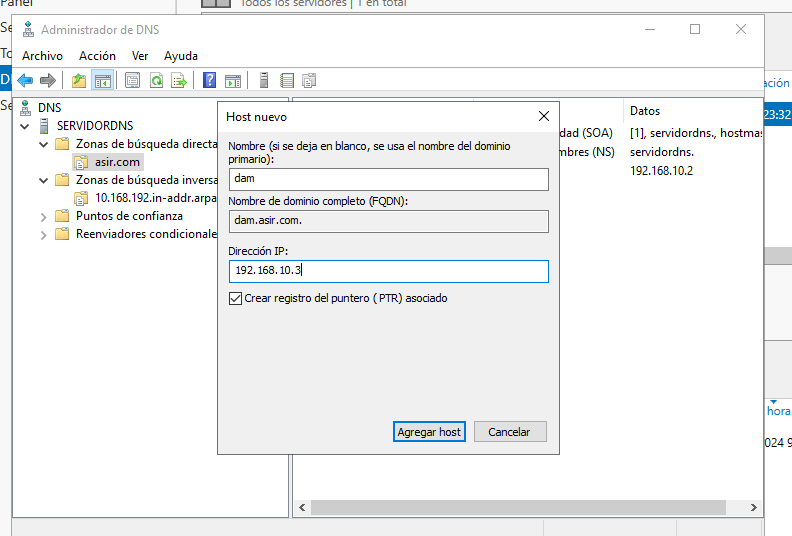
Una de las cosas más importantes es asignar el ID de la red “192.168.10” para que solo busque en la red nuestra.



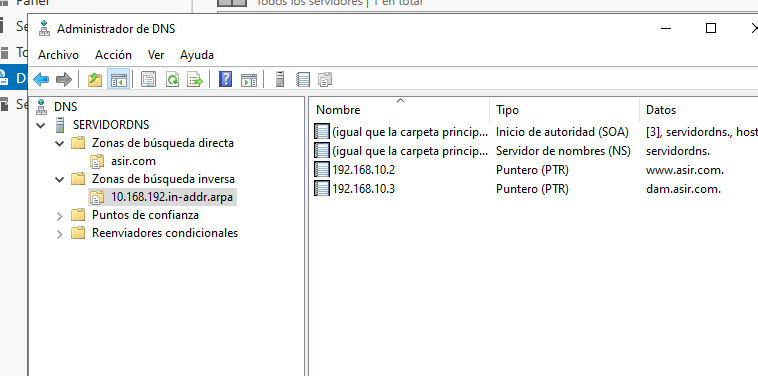
Y el nombre se lo dejamos tal cual



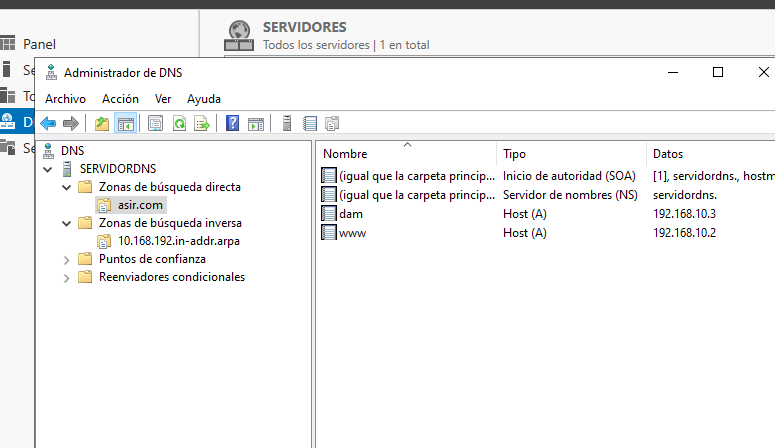
Y hacemos lo mismo también agregamos otro nuevo host en mi caso he cambiado el www por dam y le he asignado otra IP ya que es otra zona de búsqueda



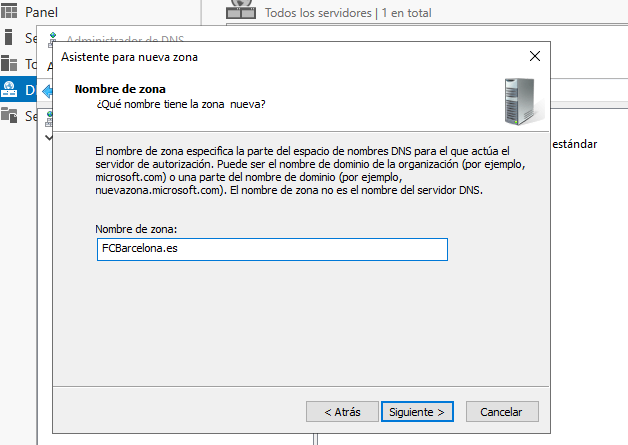
Como podemos observar en la siguiente imagen si desplegamos la zona inversa observamos los punteros PTR que son registros DNS cuya función principal es asociar la IP con un nombre de dominio en nuestro caso la 192.168.10.2/3 para www.asir.com y dam.asir.com lo que permite realizar la resolución inversa.



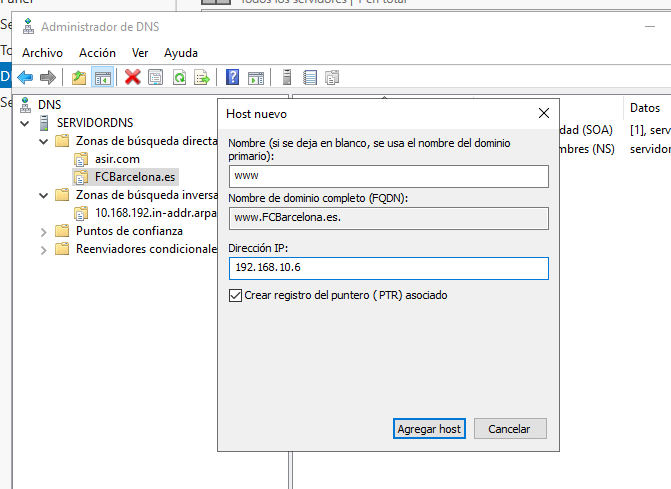
Y si desplegamos la zona de búsqueda directa nos apareces los HOST de tipo A (Adress) que son registros que vinculan un nombre de dominio con la dirección IP específica del tipo IPv4, eso permite resolver el nombre de dominio en una dirección IP.



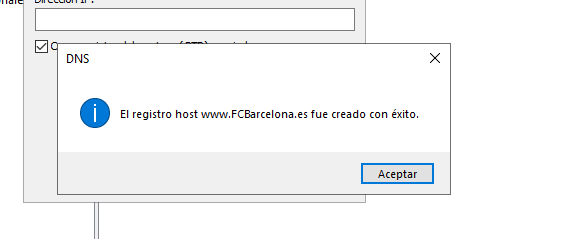
Ahora hacemos lo mismo, pero con el FCBarcelona el mejor equipo de la historia, es decir, creamos una nueva zona directa.



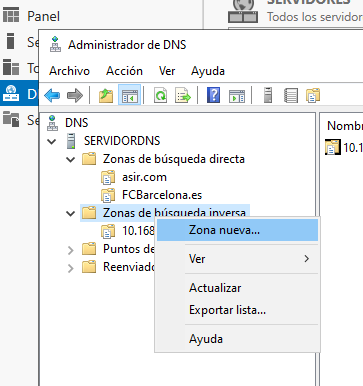
Y le asignamos un nuevo Host de tipo A con la IP 192.168.10.6 con el nombre de www.



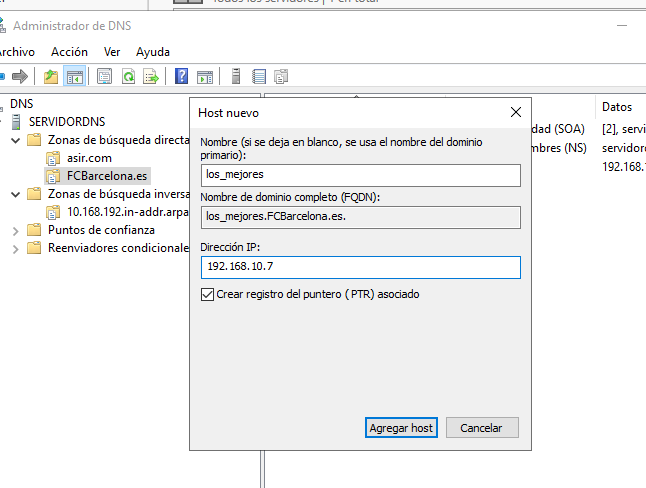
Y como se puede observar se registró correctamente



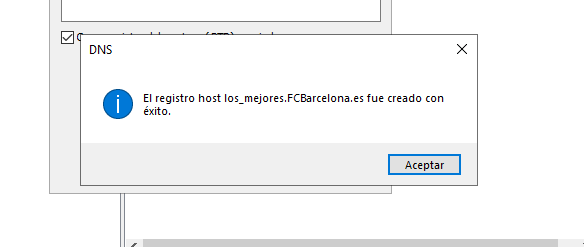
Volvemos a hacer lo mismo, pero en la zona inversa



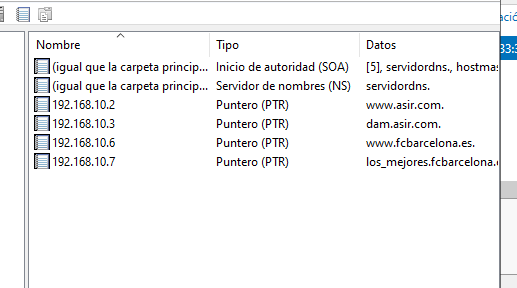
Y le asignamos un nuevo host de tipo PTR para que vincule la IP 192.168.10.7 con el nombre los\_mejores.FCBarcelona.com



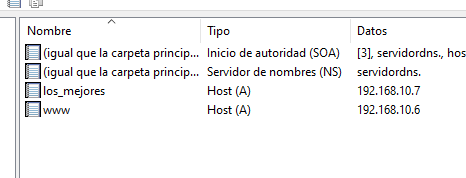
Y se ha creado correctamente el nuevo registro host



Y como podemos observar se han agregado correctamente los nuevos punteros.

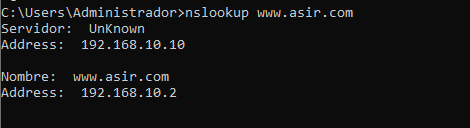


Al igual en la nueva zona directa los HOST de tipo Adress

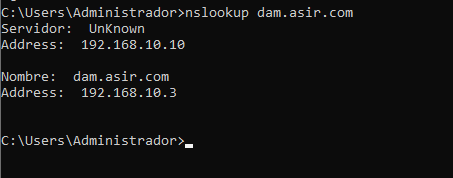


## ***Comprobaciones de zonas directas e inversas***

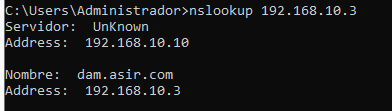
Ahora toca las comprobaciones, para ello abrimos un CMD y ejecutamos un nslookup a www,asir.com para ver si nos devuelve la IP



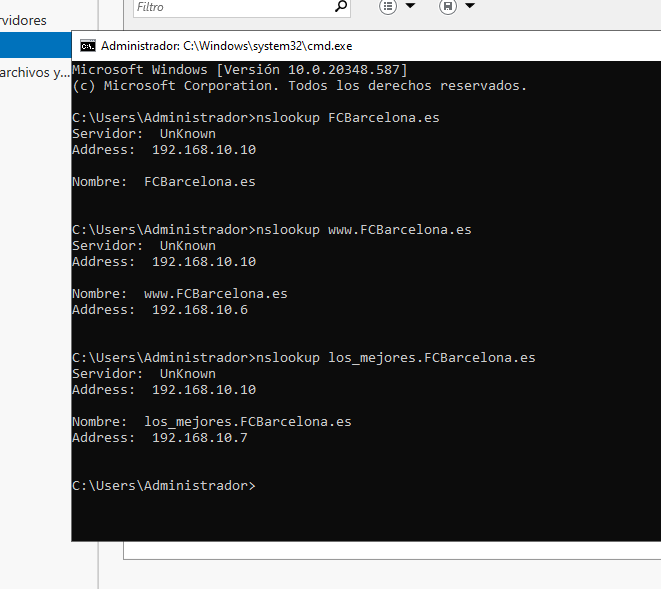
Y lo mismo con un nslookup con dam.asir.com



Una vez comprobado vemos si nos lo hace de manera inversa ejecutando un nslookup y la IP

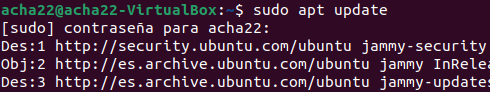
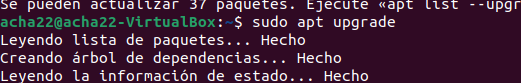


Y ahora hacemos las comprobaciones con el mejor nombre que domina al Real Madrid, en nombre de dominio FCBarcelona

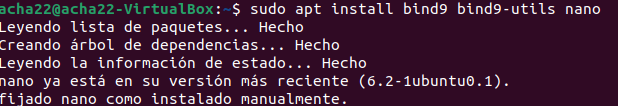


# ***Servidor DNS en Linux***

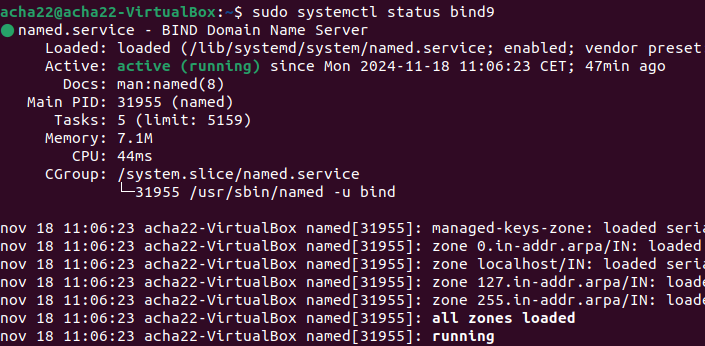
Para instalar un servidor DNS en Linux de hace con la herramienta Bind9 para ello lo primero que tenemos que hacer es actualizar los paquetes con los comandos “sudo apt update y upgrade”



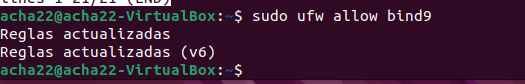
Luego instalamos el paquete Bind9 que es un software de servidor DNS que proporciona la capacidad de gestionar y resolver nombres de domino y viceversa para instalarlo utilizamos el comando “sudo apt install bind9 bind9-utils nano “



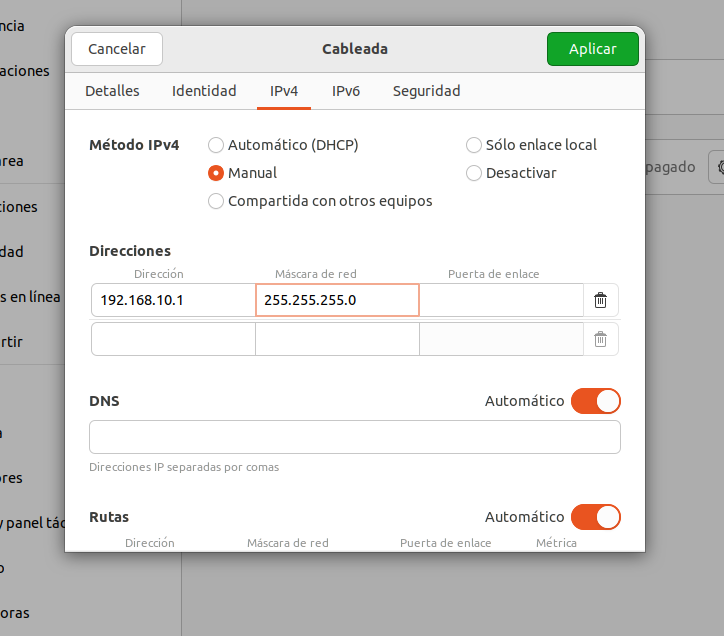
Y comprobamos el estado de nuestro servidor a la par de ver si ya se ha instalado correctamente.



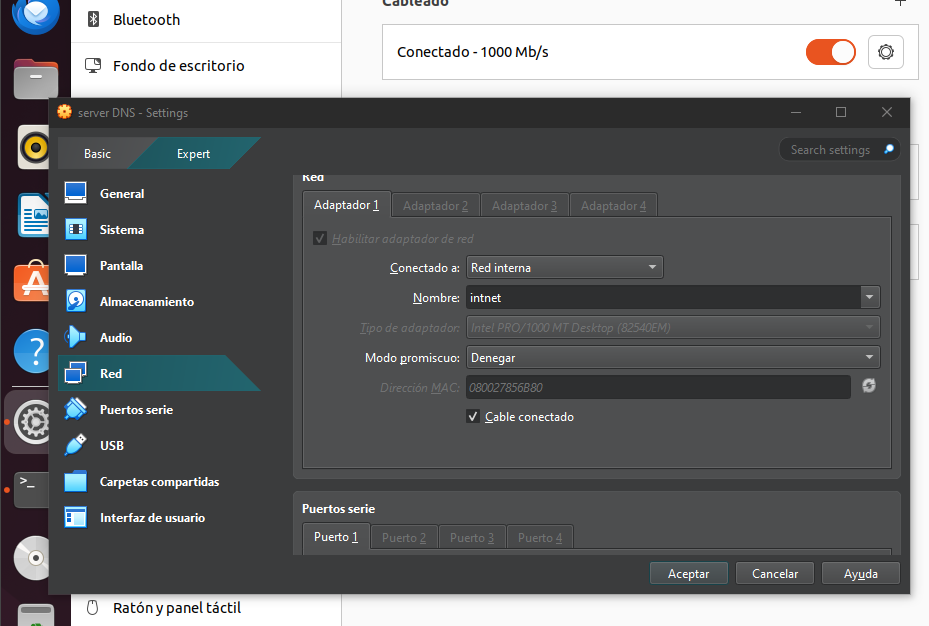
Al igual que hemos hecho en Windows tenemos que habilitar la herramienta bind 9 en Firewall para que pueda utilizar el puerto y el protocolo.



Lo que hacemos después es asignarle una IP estática a la maquina servidora en mi caso la 192.168.10.1 con mascara de red 255.255.255.0.

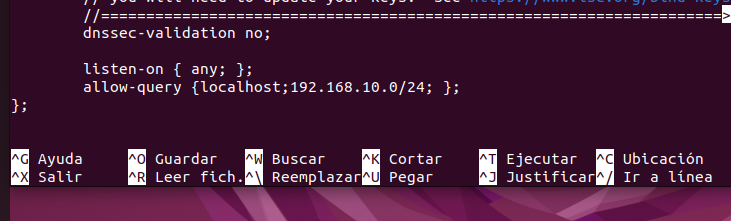


Y una vez todo instalado ya que necesitábamos conexión a la red volvemos la maquina red interna.



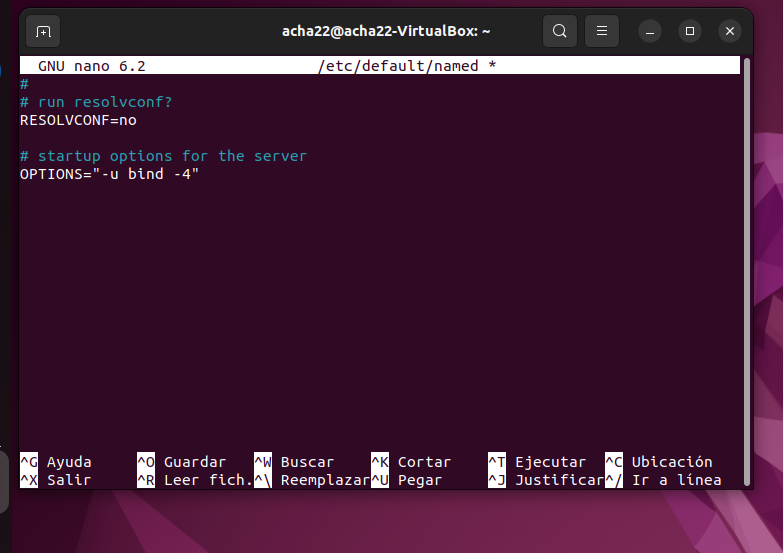
Este fragmento dentro del archivo de configuración **/etc/bind/named.conf.options** en un servidor DNS Bind9 configura varias opciones importantes:

1. **listen-on { any; };**: Hace que el servidor DNS escuche en todas las interfaces de red disponibles.
2. **allow-query { localhost; 192.168.10.0/24; };**: Permite consultas DNS solo desde localhost y la red **192.168.10.0/24**

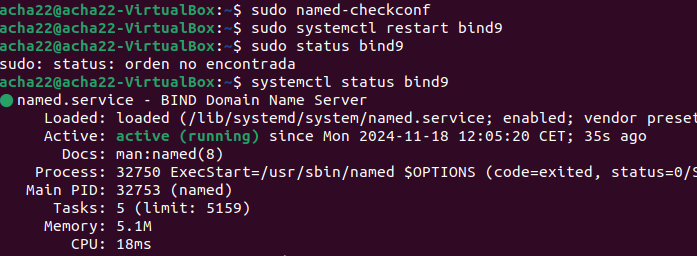


Para obligar que solo utilice el uso único de IPV4 tenemos que modificar el archivo /etc/default/named

Y le ponemos el -4 refiriéndose a IPv(4)

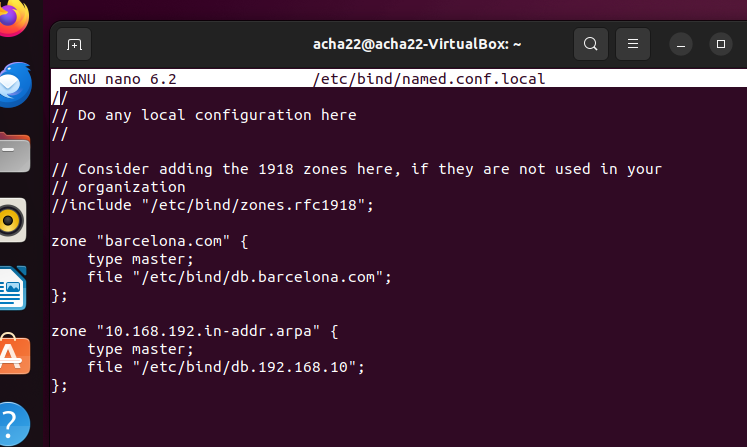


Chequeamos la configuración de bind9 con el comando sudo named-checkconf, si nos pone nada después de ejecutarlo significa que esta bien, y restauramos para que se guarden los cambios de configuración y verificamos el estado del servidor con el comando sudo systemctl status bind9



## ***Agregar zonas***

Ahora pasamos a agregar las zonas tanto directa como inversa en el archivo /etc/bind/named.conf.local y darle la url del archivo donde van a estar configuradas.



Existe un archivo a la hora que instalamos el paquete llamado db.local donde se encontraba la configuración base de las zonas y para ello copias el contenido en el nuevo archivo llamado db.barcelona.com



## ***Configuración de zonas***

Este fragmento de configuración es parte de un archivo de zona DNS.

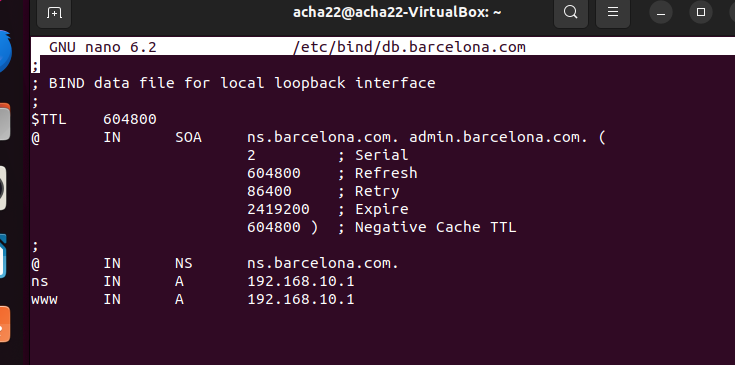
**$TTL 604800**: Establece el tiempo de vida predeterminado de los registros DNS a 604800 segundos (7 días).

* **@ IN SOA ns.barcelona.com. admin.barcelona.com.**: Define el registro SOA (Start of Authority), indicando que ns.barcelona.com es el servidor principal y admin.barcelona.com es el contacto del administrador.
* **Serial**: Número de serie que se incrementa cada vez que se realiza una modificación en el archivo.
* **Refresh**: Tiempo que los servidores secundarios esperan antes de verificar si hay cambios en el servidor principal (604800 segundos = 7 días).
* **Retry**: Tiempo que se espera antes de intentar de nuevo la actualización en caso de error (86400 segundos = 1 día).
* **Expire**: Tiempo que los servidores secundarios mantienen los registros DNS antes de eliminarlos si no pueden obtener actualizaciones del servidor principal (2419200 segundos = 28 días).
* **Negative Cache TTL**: Tiempo que los servidores DNS mantendrán en caché las respuestas negativas (sin resultados) antes de intentar una nueva consulta (604800 segundos = 7 días).

Los siguientes registros:

* **@ IN NS ns.barcelona.com.**: Define ns.barcelona.com como el servidor de nombres autoritativo para la zona barcelona.com.
* **ns IN A 192.168.10.1**: Asocia ns.barcelona.com con la dirección IP 192.168.10.1.
* **www IN A 192.168.10.1**: Asocia www.barcelona.com con la misma dirección IP 192.168.10.1.

Este archivo configura el servidor DNS para que resuelva correctamente los nombres de dominio dentro de la zona barcelona.com.

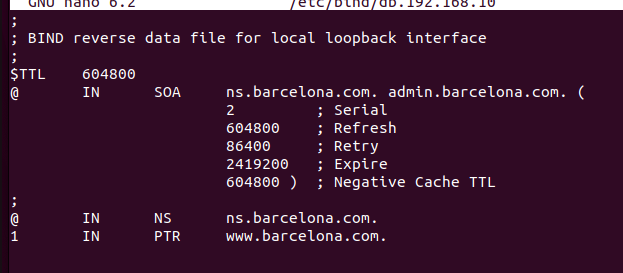


Hacemos lo mismo con el archivo de zona inversa que hemos llamado db.192.168.10

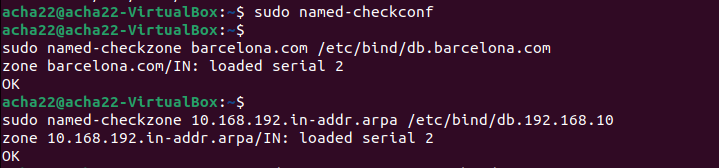


Este fragmento configura una zona DNS para barcelona.com:

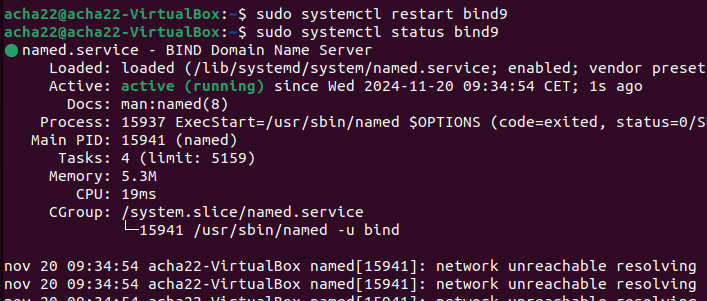
* **$TTL 604800**: Tiempo de vida de 7 días para los registros.
* **@ IN SOA**: Define el registro SOA, donde ns.barcelona.com es el servidor de nombres y admin.barcelona.com es el administrador.
* **Serial**: Número de serie de la configuración.
* **@ IN NS ns.barcelona.com**: Especifica el servidor de nombres autoritativo.
* **1 IN PTR www.barcelona.com.**: Asocia la IP 1 con el nombre www.barcelona.com en la zona inversa.



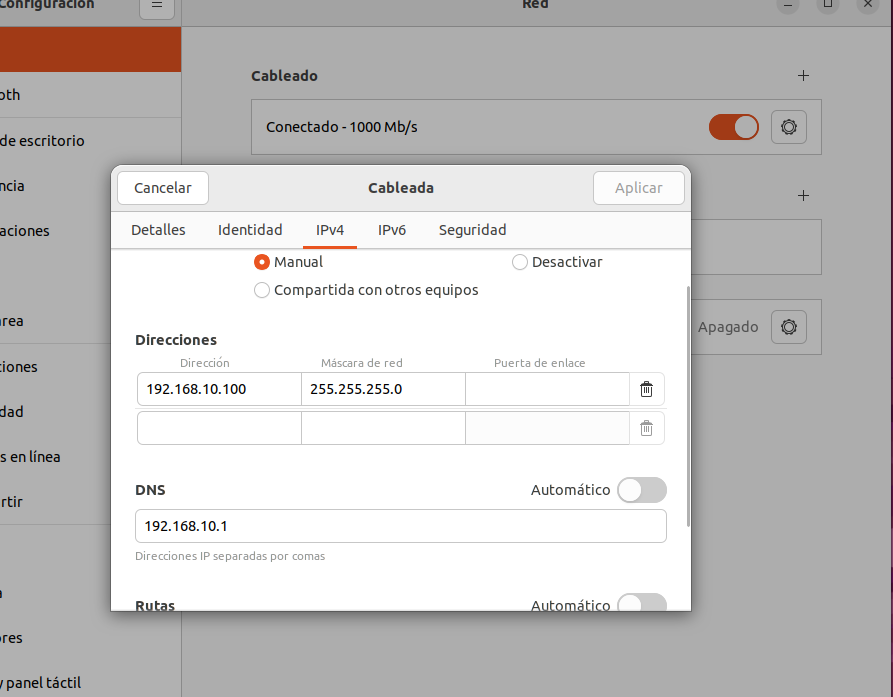
Volvemos a chequear la configuración del servidor y también de las zonas si nos pone un OK es que están bien configuradas.



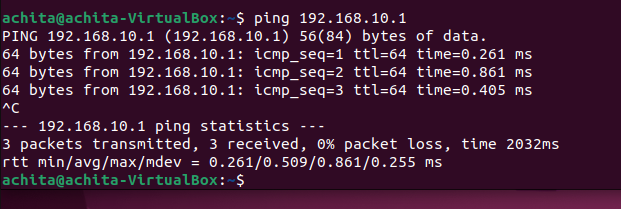
Una vez todo configurado restauramos el sistema para que se guarden los cambiaos y comprobamos el estado del servidor.



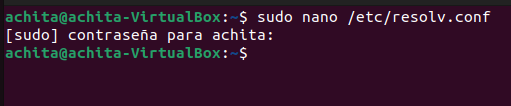
Al comprobar que no tenemos ningún fallo en el servidor nos dirigimos a la configuración de red la maquina le asignamos una IP estática en mi caso la 192.168.100 y en el DNS le asignamos la IP de nuestro servidor la 192.168.10.1

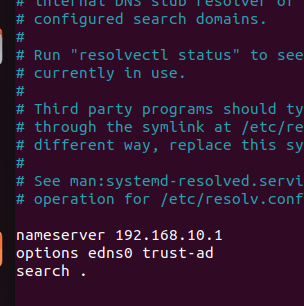


Comprobamos que la maquinas están en la misma red y hacen ping entre ellas



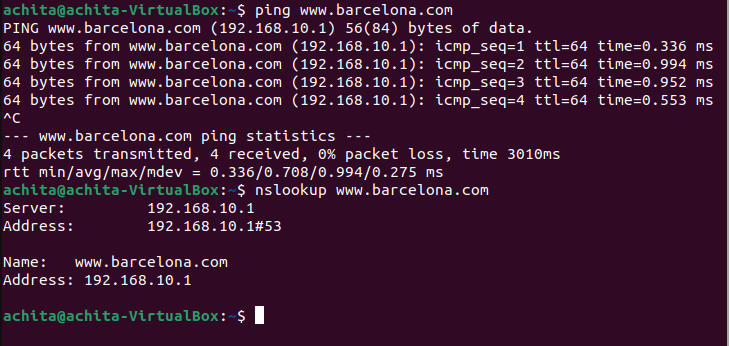
El archivo /etc/resolv.conf en Linux se utiliza para configurar los servidores DNS que el sistema emplea para resolver nombres de dominio. Contiene directivas como nameserver, que especifica las direcciones IP de los servidores DNS que en nuestro caso pusimos las de nuestro servidor , y search o domain para la búsqueda de dominios. Es esencial para que el sistema realice correctamente las consultas de nombres y se conecte a recursos en la red.



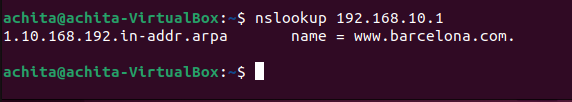


## ***Comprobación de zonas***

Para final ya podemos comprobar lo realizado anteriormente como se puede observar si hacemos un ping a www.barcelona,com nos hace ping y además nos devuelve la IP y con el nslookup nos lo especifica mejor hasta nos dice el puerto por el que se comunica el 53 ya que el dns se comunica por el 53/UDP y TCP.



Ahora comprobamos la zona inversa ejecutado el nslookup, pero con la IP y nos tiene que devolver el nombre de dominio como en este caso,



## ***Conclusión***

La implementación de un servidor DNS en Linux o Windows es esencial para garantizar una resolución eficiente de nombres dentro de una red. Este sistema permite la asociación entre nombres de dominio y direcciones IP mediante zonas de búsqueda directa (nombre a IP) e inversa (IP a nombre). Ambas configuraciones son fundamentales para el funcionamiento de servicios como el correo electrónico o el acceso a sitios web internos.

**Servidor DNS en Linux (Bind9):**

* **Zonas de búsqueda directa**: se definen en archivos como /etc/bind/db.nombredominio, asignando nombres de dominio a direcciones IP.
* **Zonas de búsqueda inversa**: se almacenan en archivos como /etc/bind/db.red, asignando direcciones IP a nombres de dominio mediante el formato **PTR**.

La administración incluye herramientas como named-checkzone y named-checkconf, que verifican la coherencia de las configuraciones antes de desplegar los cambios.

**Servidor DNS en Windows (DNS Server):**

En Windows, el servidor DNS se gestiona mediante interfaces gráficas en el **Administrador del Servidor**. Este enfoque facilita la creación de:

* **Zonas de búsqueda directa**, que asocian nombres a IPs a través de asistentes.
* **Zonas inversas**, que permiten resolver direcciones IP a nombres y son útiles en autenticaciones o diagnóstico

Ambos sistemas son robustos y se ajustan a necesidades específicas. Linux, mediante Bind9, destaca por su personalización y uso en servidores de alta demanda. Por otro lado, Windows ofrece simplicidad e integración en redes corporativas.