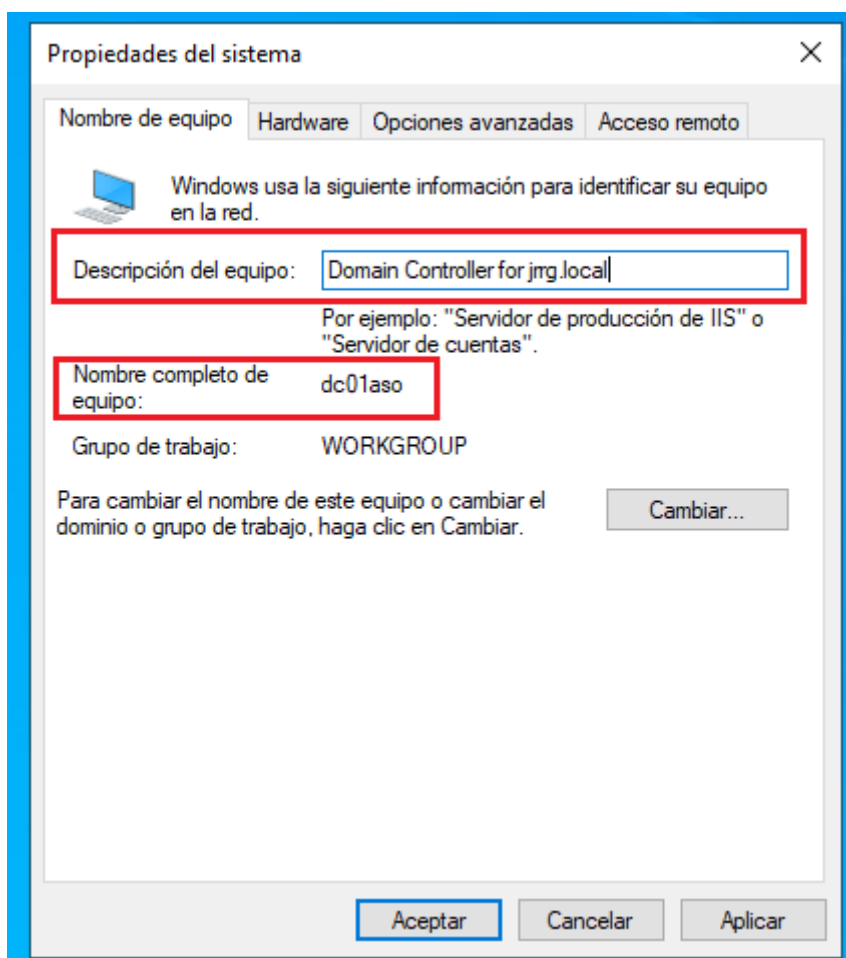
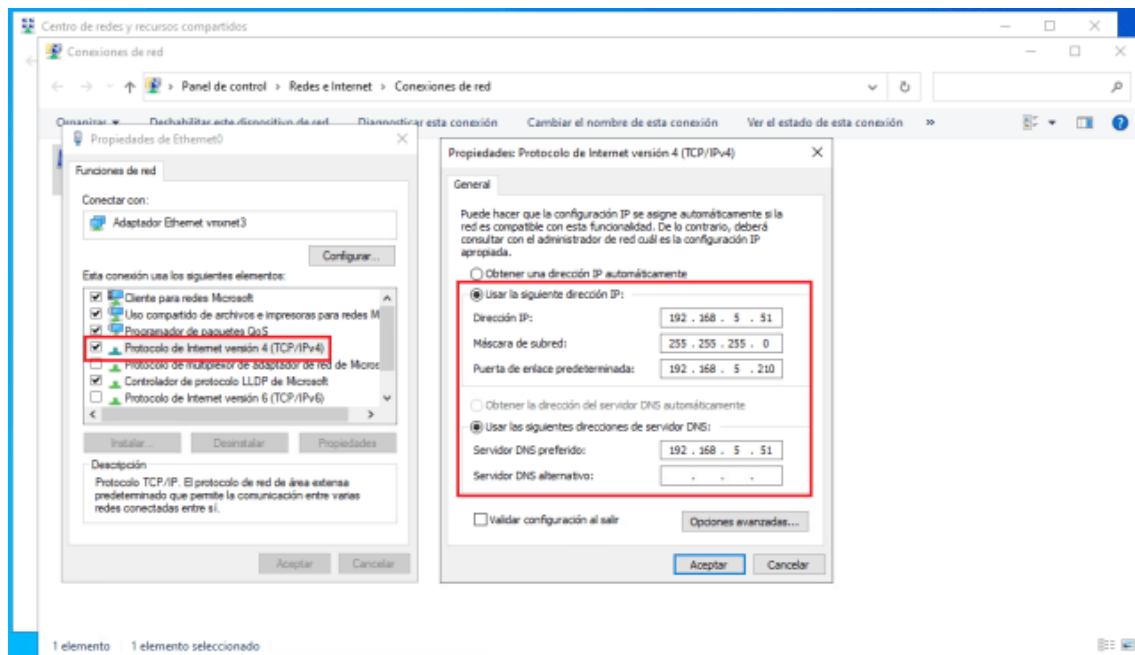


Instalar y configurar Active Directory Domain Services en Windows Server 2022.



Empezamos la configuración de nuestro controlador de dominio asignándole un nombre y una dirección IP estática, y como DNS le asignamos su propia dirección IP, ya que se encargará de toda la gestión DNS de nuestro entorno:

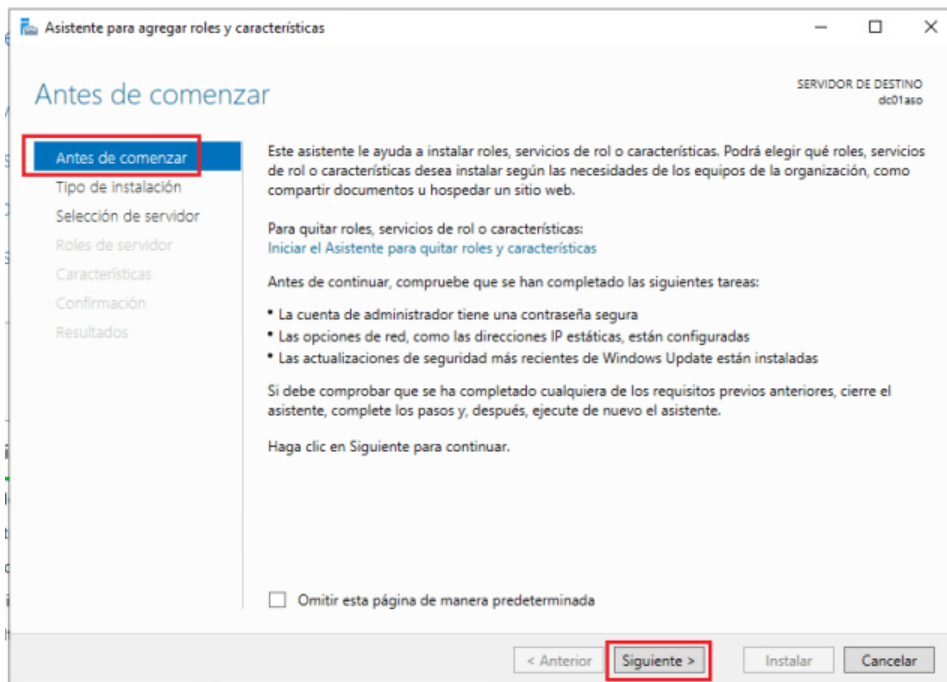




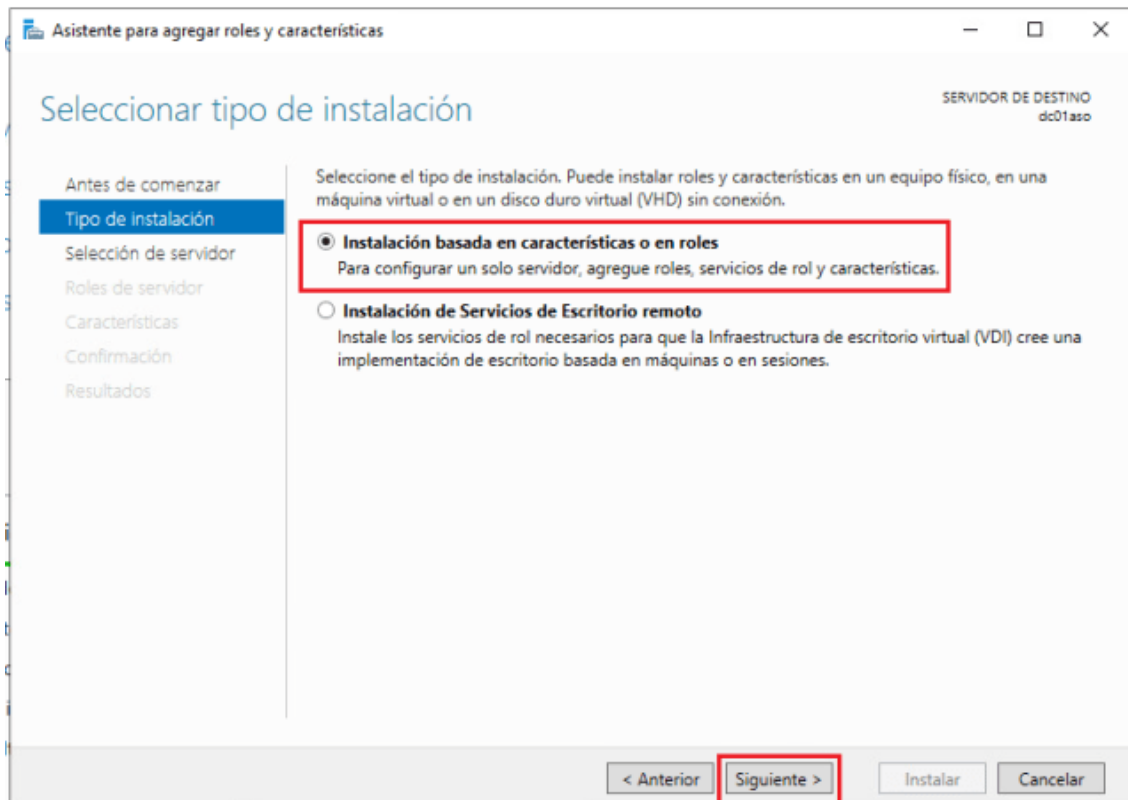
- Abrimos el Administrador del servidor y agregamos roles y características:



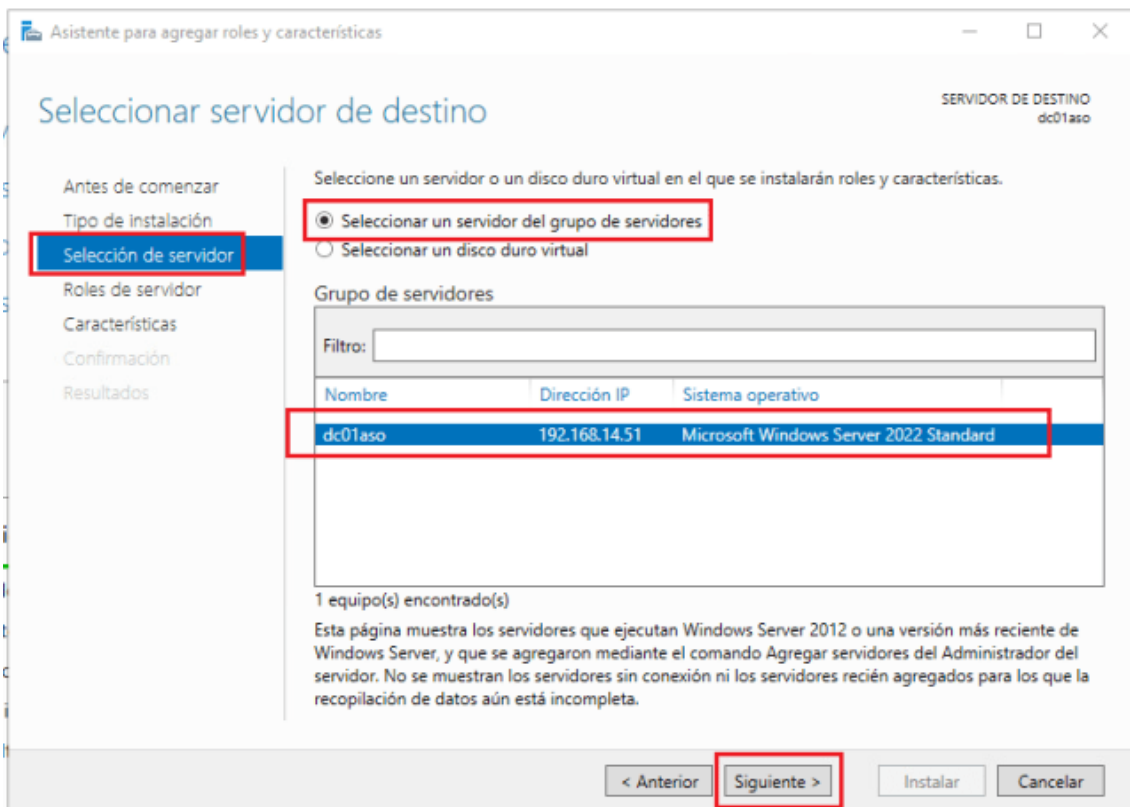
- Se nos abre el siguiente asistente, clic en siguiente:



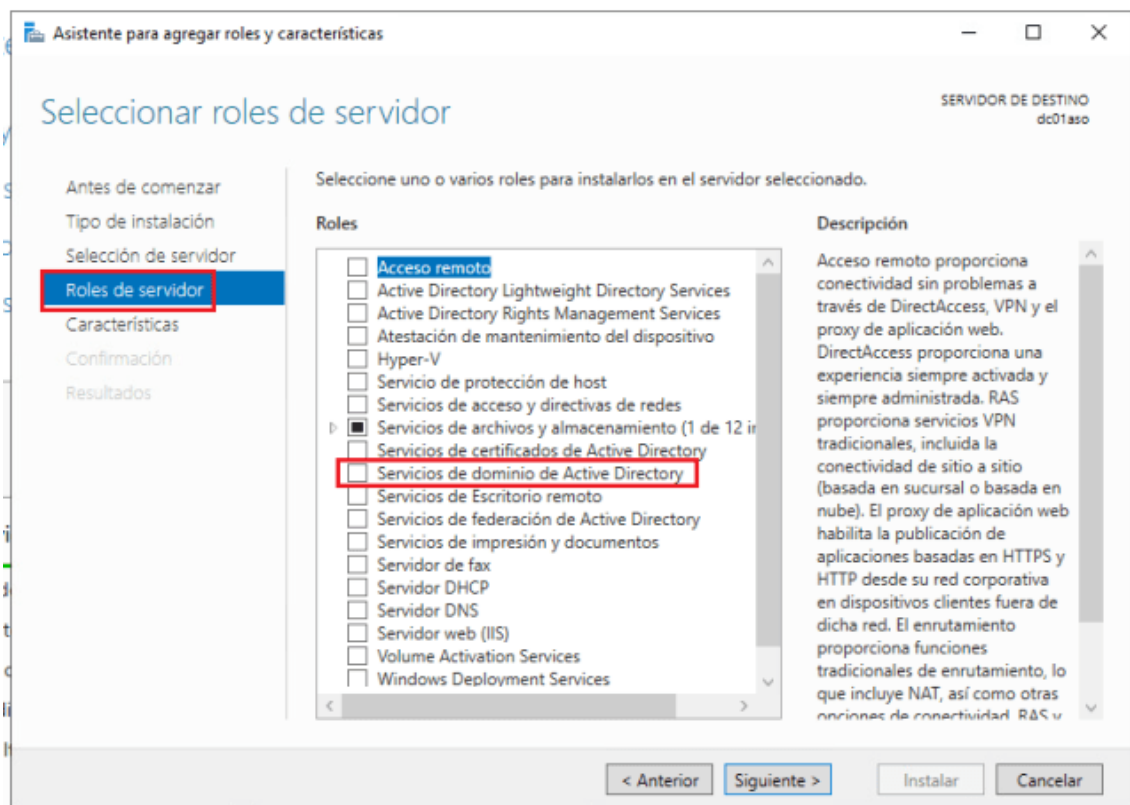
- Elegimos la opción instalación basada en características o roles:



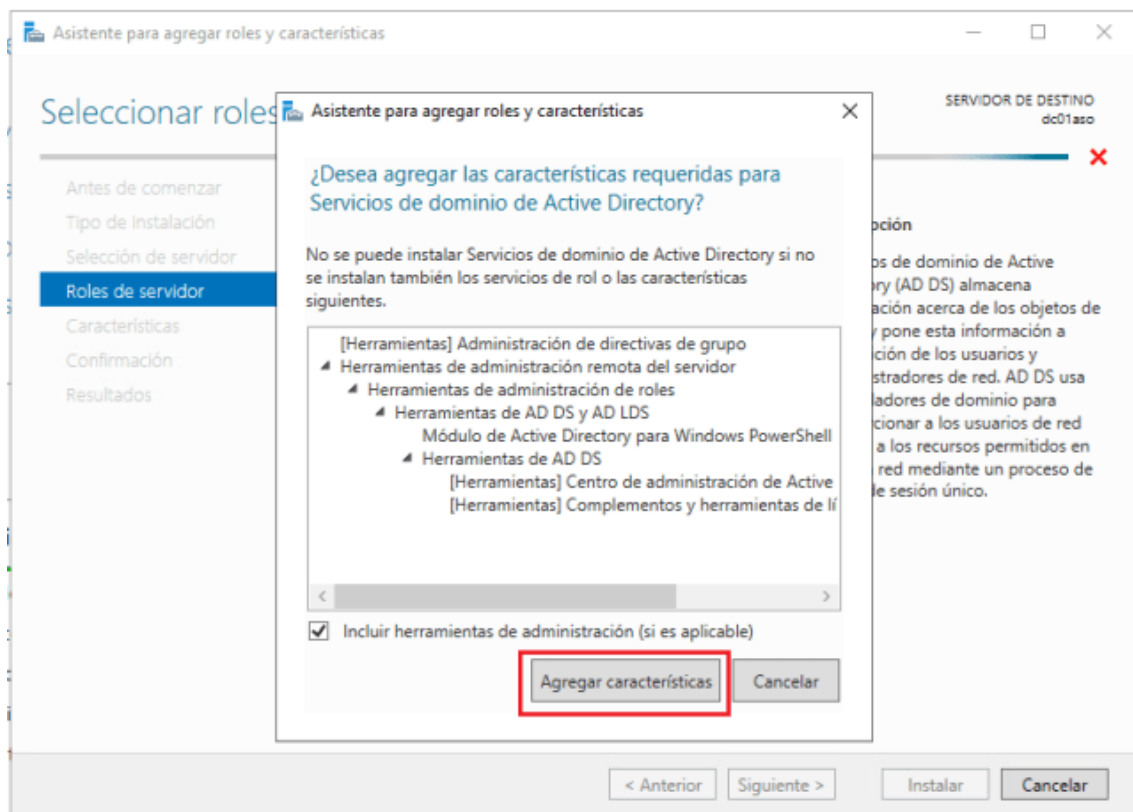
- Seleccionamos nuestro servidor dc01aso:



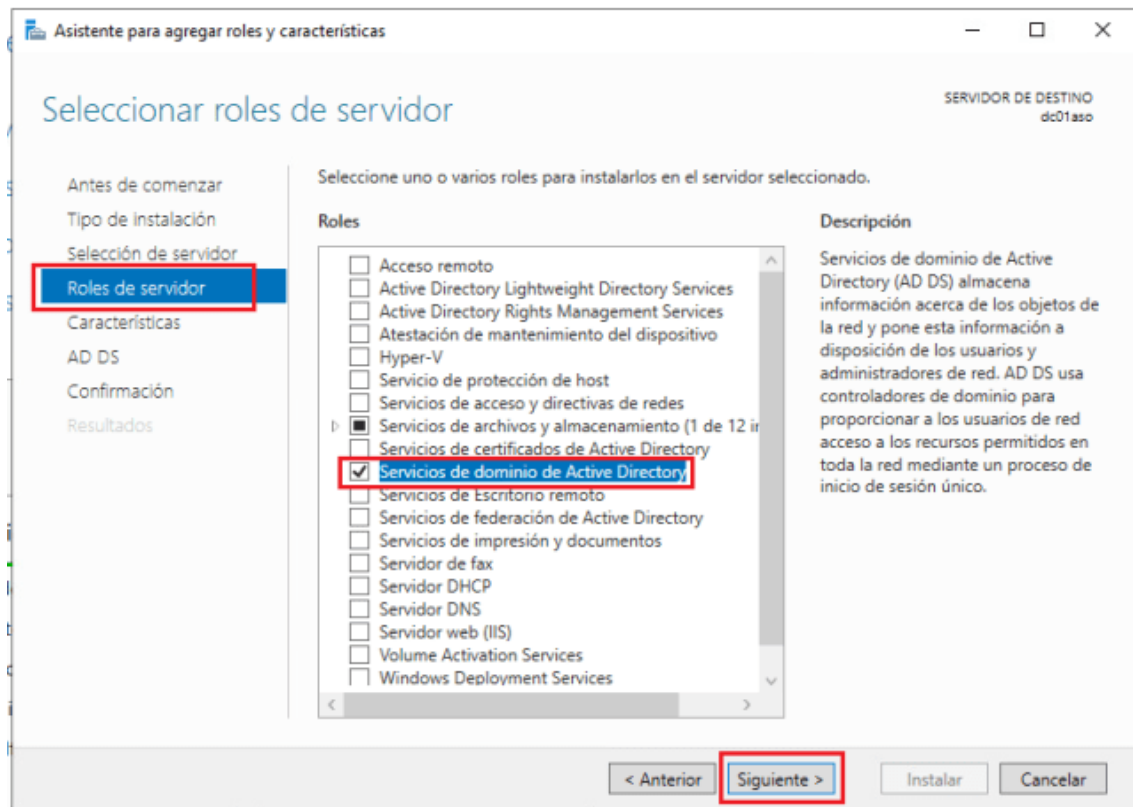
- Ahora agregamos el rol de Servicios de dominio de Active Directory:



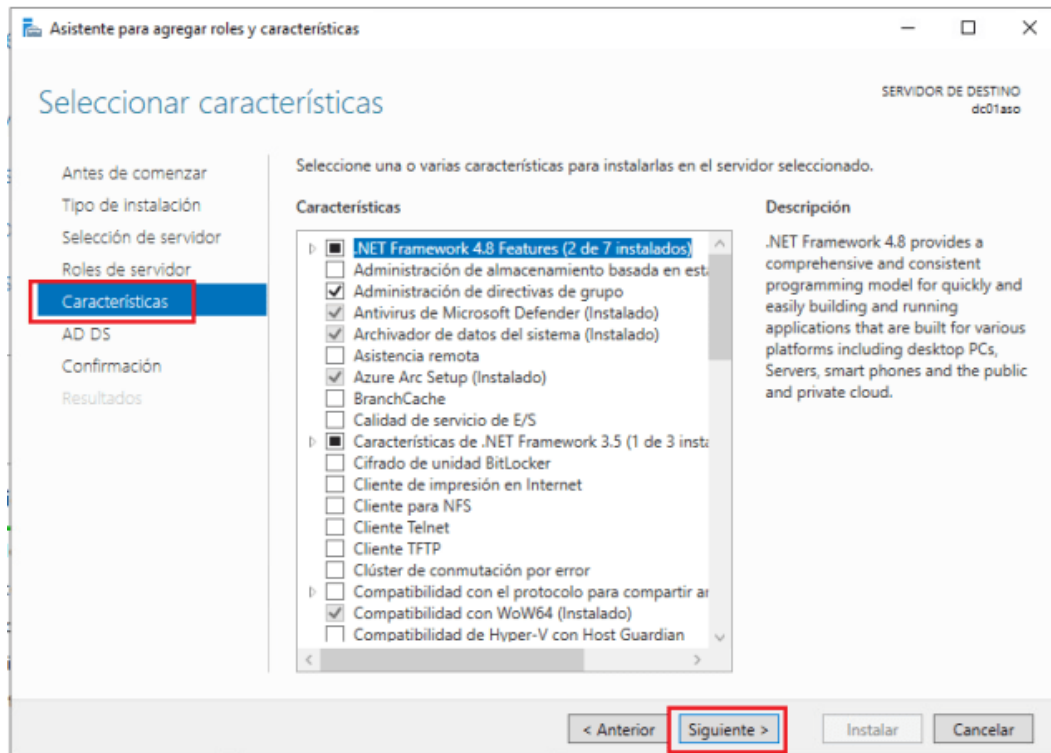
- Agregamos las características:



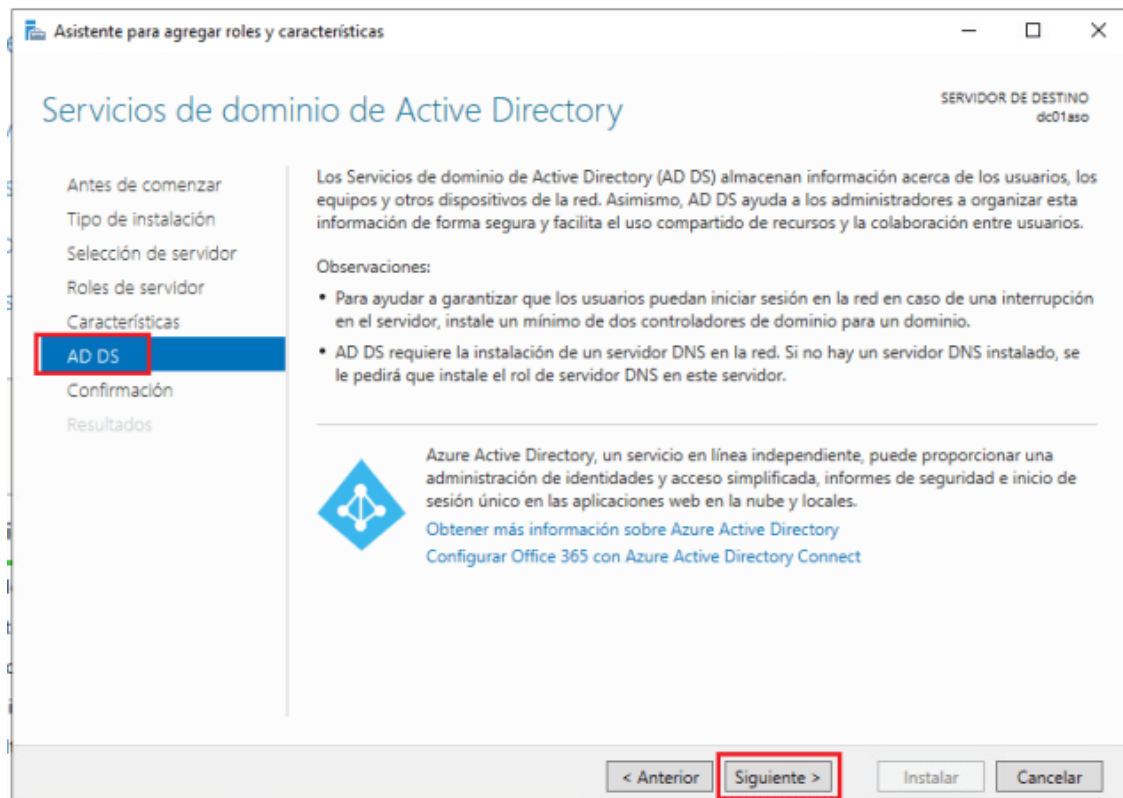
- Continuamos con la instalación del rol:



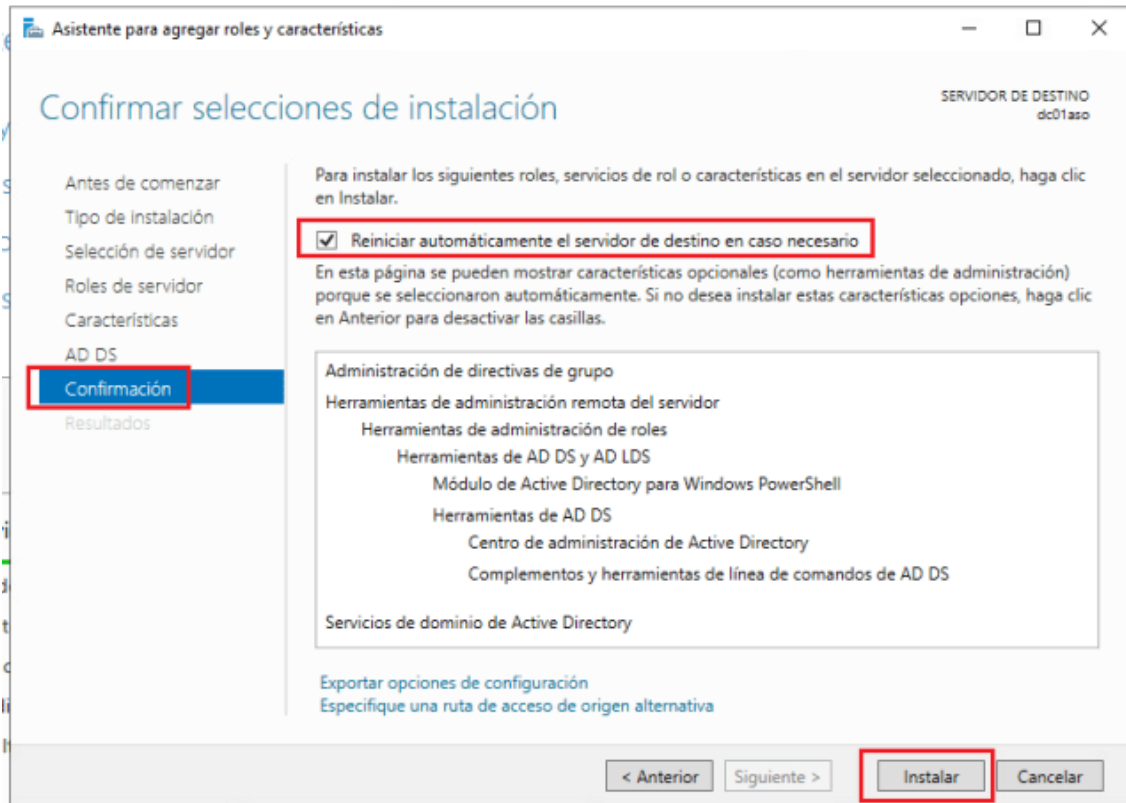
- Todas las características que requiere nuestro controlador de dominio de Active Directory se seleccionan por defecto por lo que hacemos clic en siguiente:



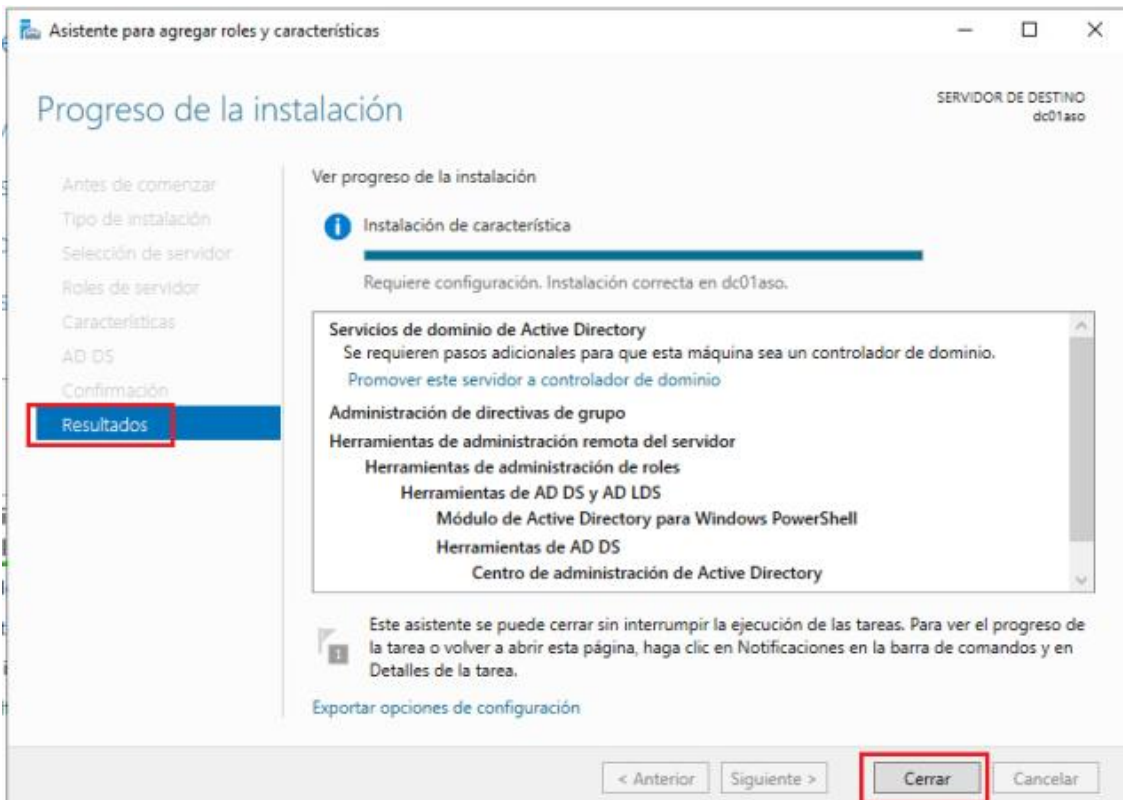
- Aquí nos muestra información sobre Active Directory, clic en siguiente:



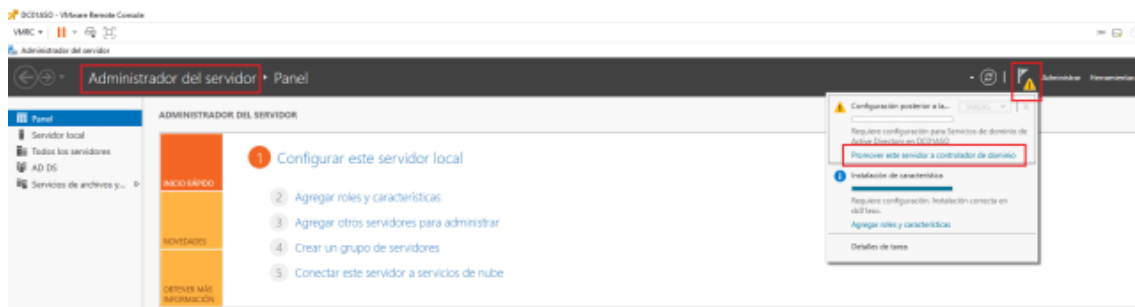
- Iniciamos el despliegue de la función Servicios de dominio de Active Directory, clic sobre “Instalar”:



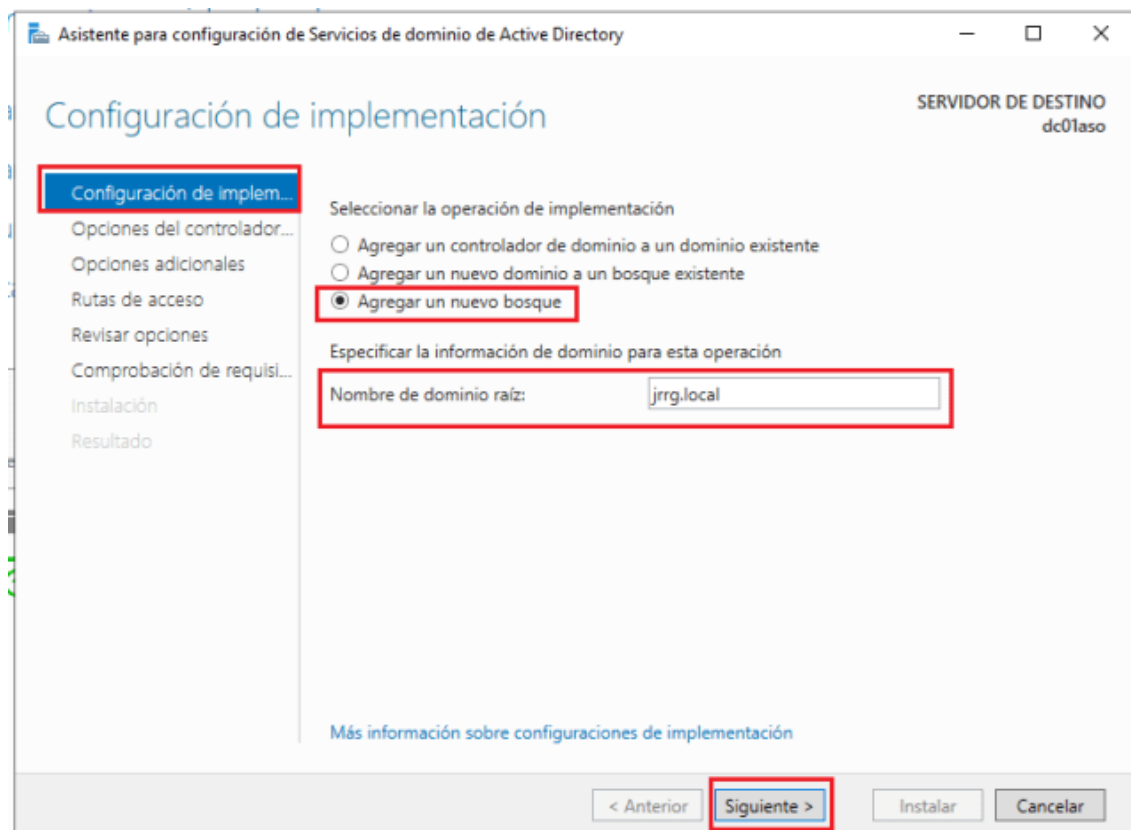
- Una vez finalizada la instalación cerramos y reiniciamos nuestro controlador de dominio:



- Tras el reinicio nos abrimos el Administrador del servidor y promovemos este servidor a controlador de dominio:



- Se nos abre el siguiente asistente y añadimos un nuevo bosque, ya que este es nuestro primer controlador de dominio en la infraestructura, escribimos nuestro nombre de dominio raíz:



- Seleccionamos el nivel funcional de nuestro bosque, en este caso Windows Server 2016, ya que no tenemos otros controladores de dominio sobre Windows Server 2003, 2008 o 2012. También seleccionamos la función de DNS en la que apoyaremos toda la infraestructura de nombres de nuestra red, aparte de que es un requisito imprescindible para Active Directory, luego introducimos una contraseña segura

que será necesaria en caso de restauración de Active Directory:

Asistente para configuración de Servicios de dominio de Active Directory

SERVIDOR DE DESTINO
dc01aso

Opciones del controlador de dominio

Configuración de Implem...
Opciones del controlador...
Opciones de DNS
Opciones adicionales
Rutas de acceso
Revisar opciones
Comprobación de requisi...
Instalación
Resultado

Seleccionar nivel funcional del nuevo bosque y dominio raíz

Nivel funcional del bosque: Windows Server 2016
Nivel funcional del dominio: Windows Server 2016

Especificar capacidades del controlador de dominio

☒ Servidor de Sistema de nombres de dominio (DNS)
☒ Catálogo global (GC)
☐ Controlador de dominio de solo lectura (RODC)

Escribir contraseña de modo de restauración de servicios de directorio (DSRM)

Contraseña:
Confirmar contraseña:

Más información sobre opciones del controlador de dominio

< Anterior **Siguiendo >** Instalar Cancelar

- Windows no puede encontrar una delegación para el servidor DNS ya que éste es el primer bosque de nuestro entorno, hacemos clic en siguiente:

Asistente para configuración de Servicios de dominio de Active Directory

SERVIDOR DE DESTINO
dc01aso

Opciones de DNS

Configuración de Implem...
Opciones del controlador...
Opciones de DNS
Opciones adicionales
Rutas de acceso
Revisar opciones
Comprobación de requisi...
Instalación
Resultado

No se puede crear una delegación para este servidor DNS porque la zona principal autoritativa no se encu... Mostrar más

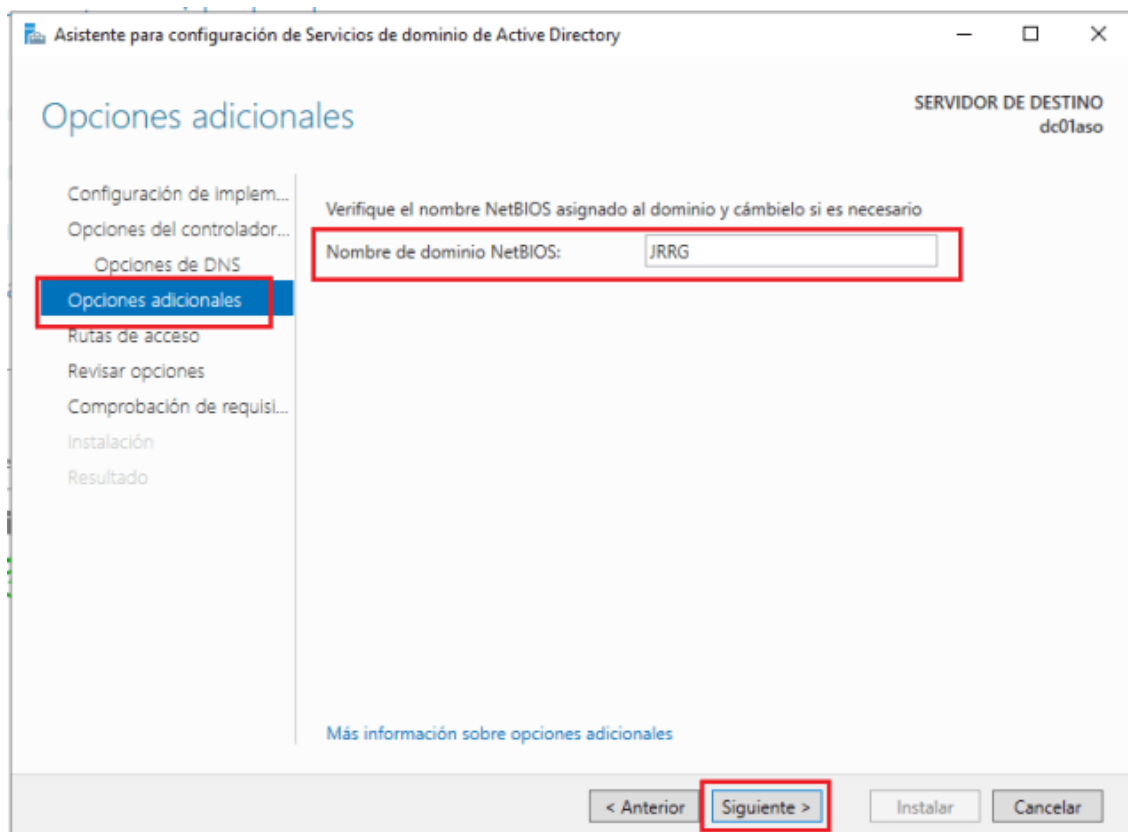
Especificar opciones de delegación DNS

☐ Crear delegación DNS

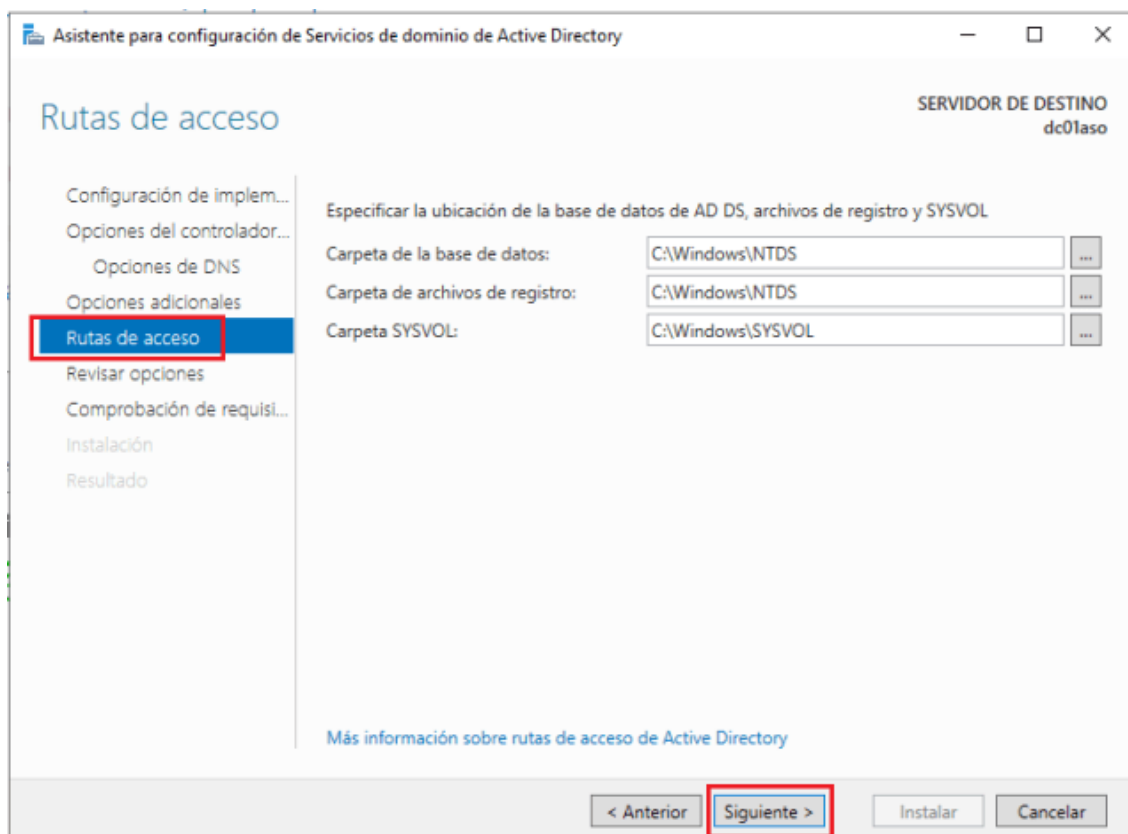
Más información sobre delegaciones DNS

< Anterior **Siguiendo >** Instalar Cancelar

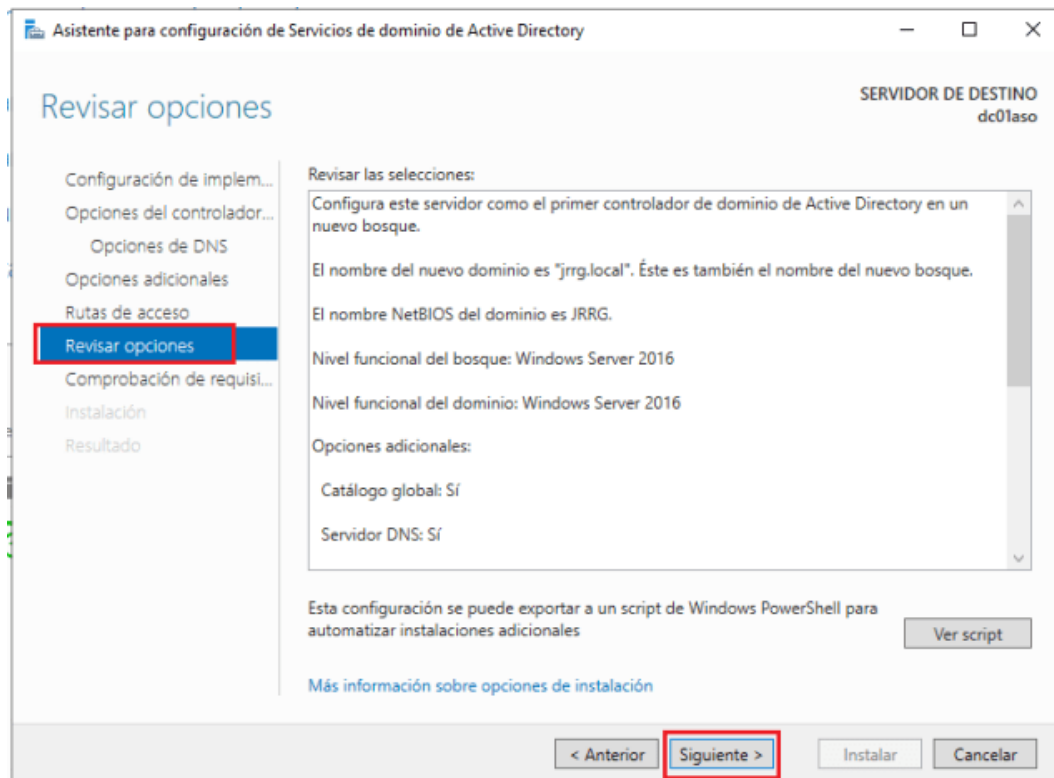
- Agregamos el nombre NETBIOS:



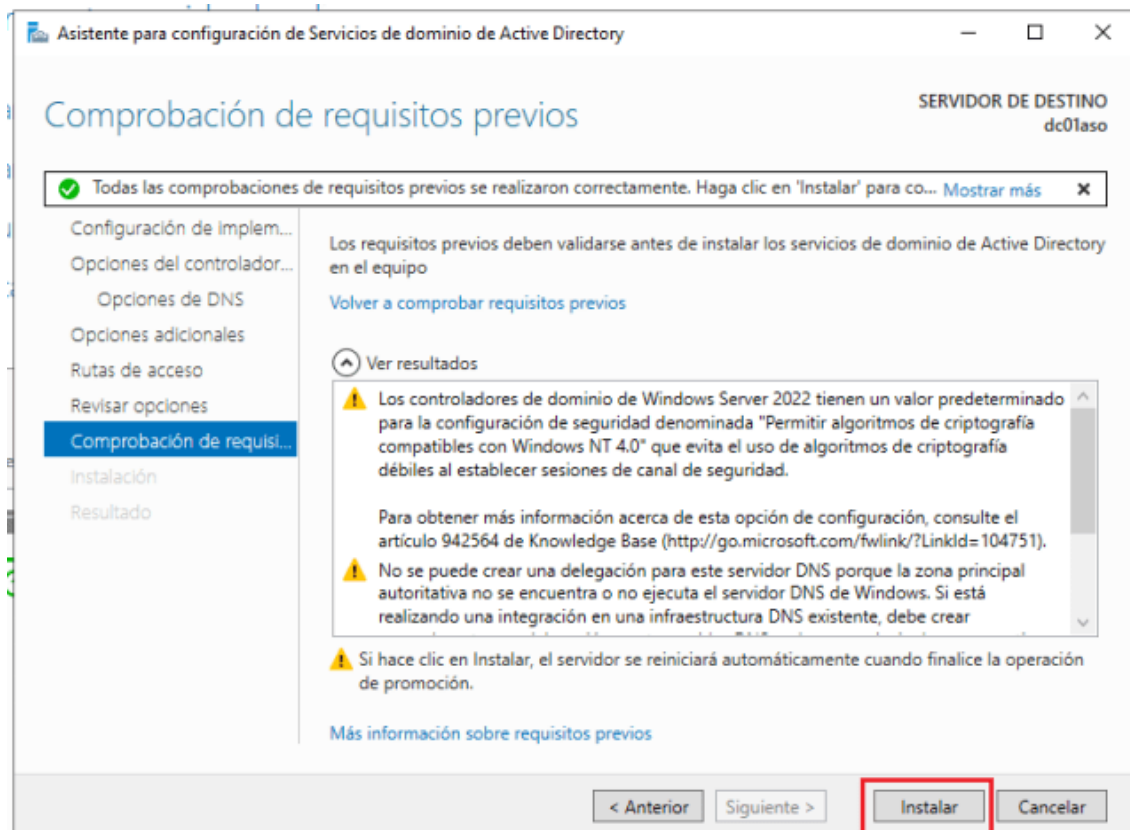
- Las rutas de acceso las dejamos por defecto:



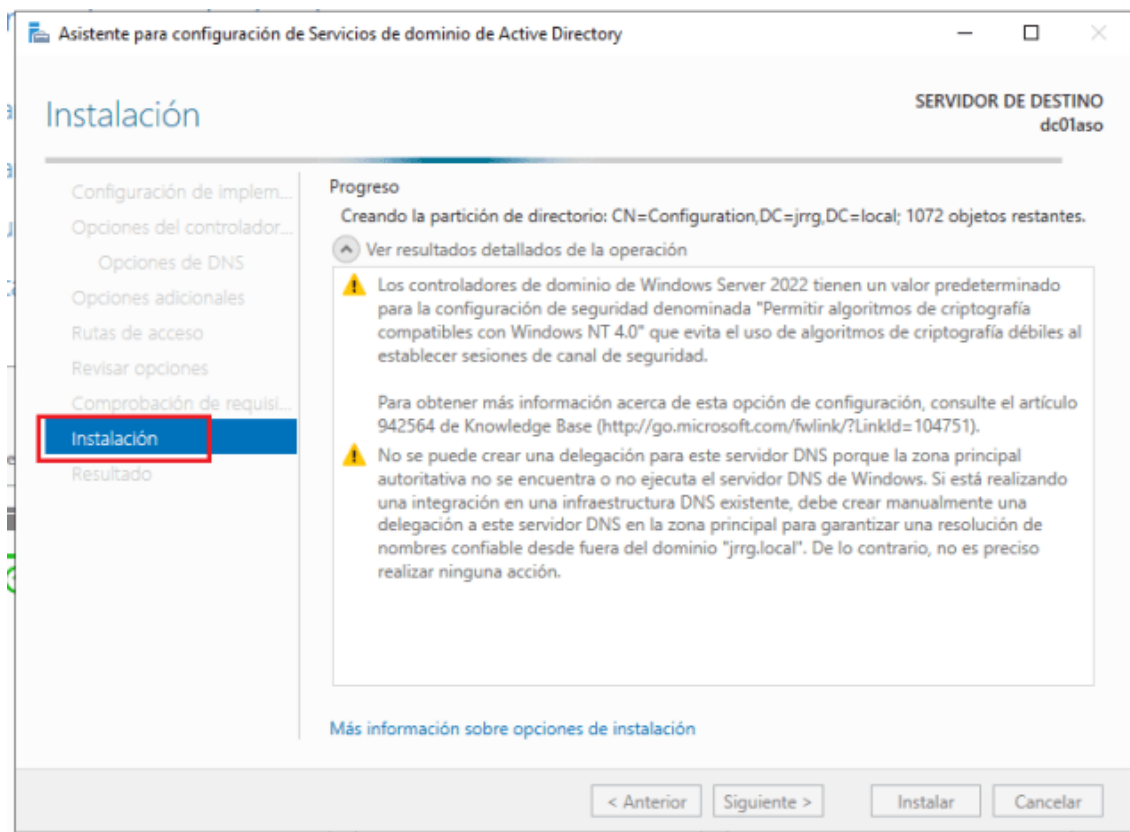
- Nos muestra un resumen de las opciones configuradas:



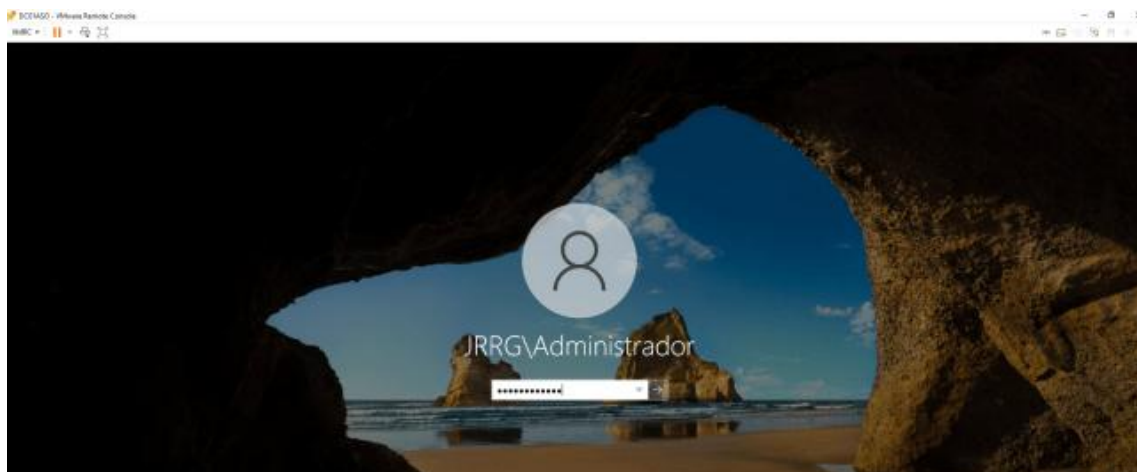
- Vemos que la comprobación de los requisitos previos está correcta, clic sobre Instalar:



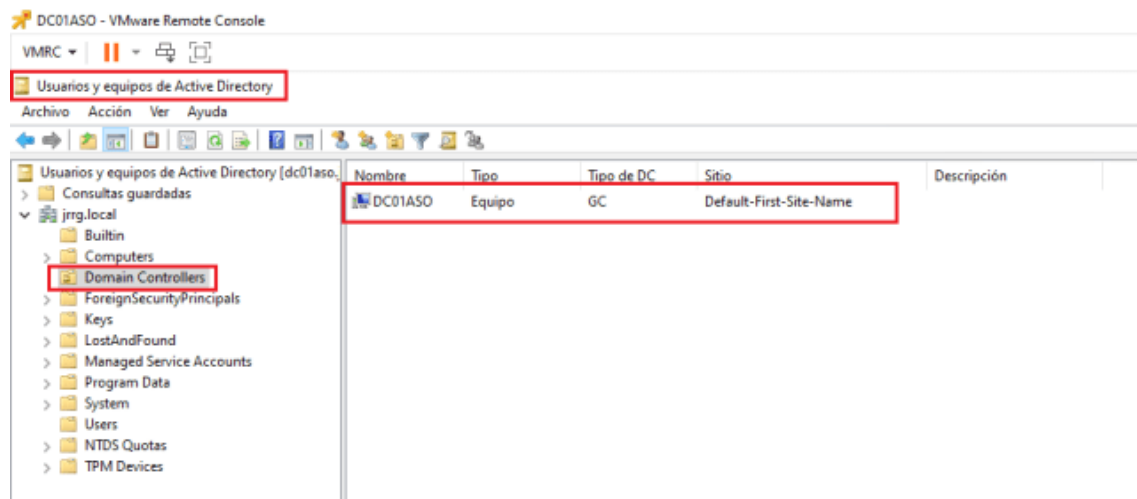
- Comienza el proceso de instalación y promoción a controlador de dominio:



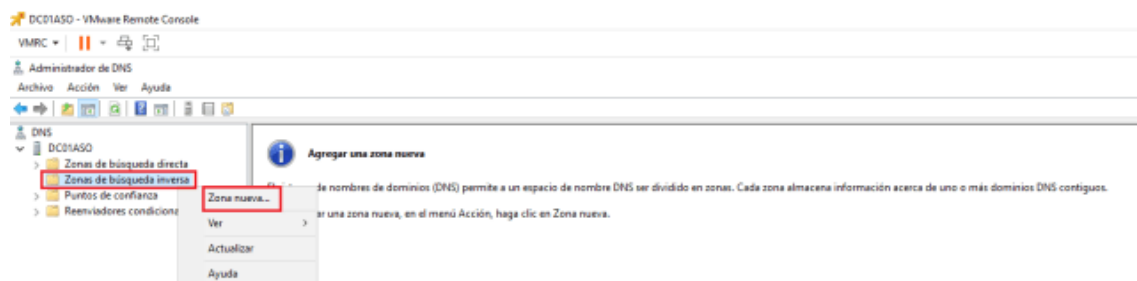
- Una vez que la instalación termina, nuestro servidor se reinicia automáticamente, y tras el reinicio, introducimos las credenciales de Administrador que será la cuenta del administrador del dominio:



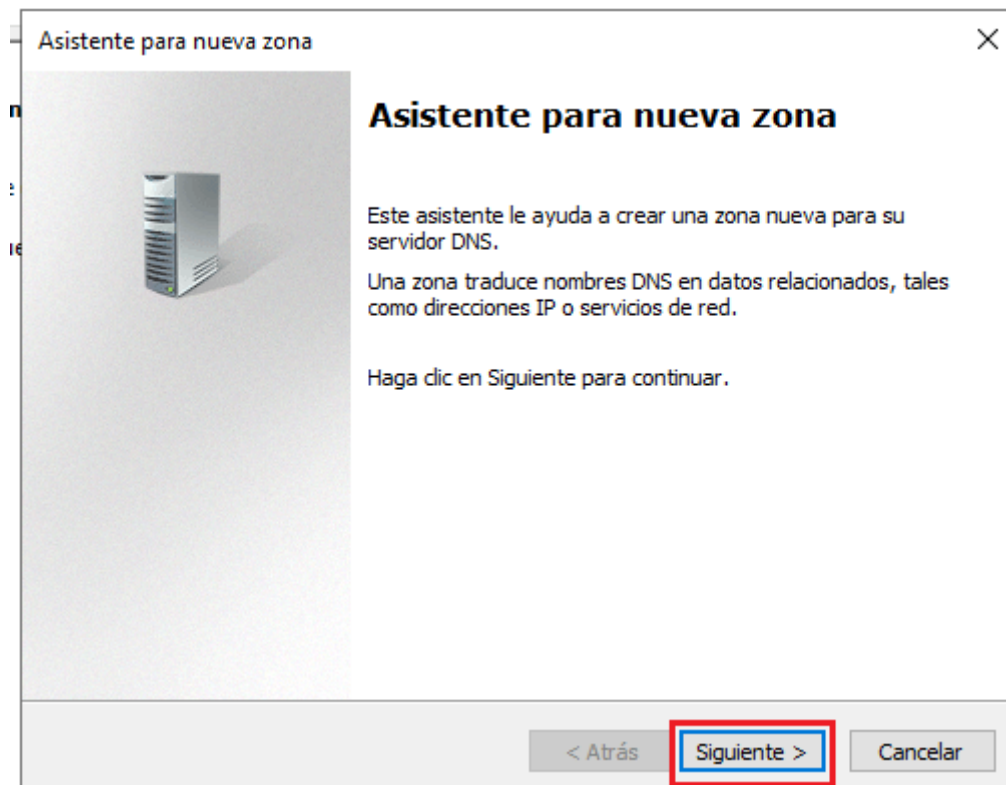
- Con esto ya tendríamos nuestro servidor promovido a controlador de dominio:



- Ahora vamos a abrir la consola de DNS y agregamos una zona nueva para la resolución inversa:



- Vamos configurando el asistente con los siguientes parámetros:



Asistente para nueva zona

Tipo de zona
El servidor DNS es compatible con varios tipos de zonas y almacenamientos.

Seleccione el tipo de zona que quiere crear:

☒ Zona principal
Crea una copia de una zona que puede actualizarse directamente en este servidor.

☐ Zona secundaria
Crea una copia de una zona que ya existe en otro servidor. Esta opción ayuda a equilibrar el proceso de carga de los servidores principales y proporciona tolerancia a errores.

☐ Zona de rutas internas
Crea una copia de zona que contiene solo servidor de nombres (NS), inicio de autoridad (SOA) y quizá registros de adherencia de host (A). Un servidor que contiene una zona de rutas internas no tiene privilegios sobre dicha zona.

☒ Almacenar la zona en Active Directory (solo disponible si el servidor DNS es un controlador de dominio grabable)

< Atrás **Siguiente >** Cancelar

Asistente para nueva zona

Ámbito de replicación de zona de Active Directory
Puede seleccionar cómo desea que se repliquen los datos DNS por la red.

Seleccione cómo quiere que se repliquen los datos de zona:

☐ Para todos los servidores DNS que se ejecutan en controladores de dominio en este bosque: jrrg.local

☒ Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio: jrrg.local

☐ Para todos los controladores de dominio en este dominio (para compatibilidad con Windows 2000): jrrg.local

☐ Para todos los controladores de dominio especificados en el ámbito de esta partición de directorio:

< Atrás **Siguiente >** Cancelar

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 **Siguiente >** Cancelar

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:

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:

< Atrás **Siguiente >** Cancelar


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

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: 5.168.192.in-addr.arpa

Tipo: Zona primaria integrada de Active Directory

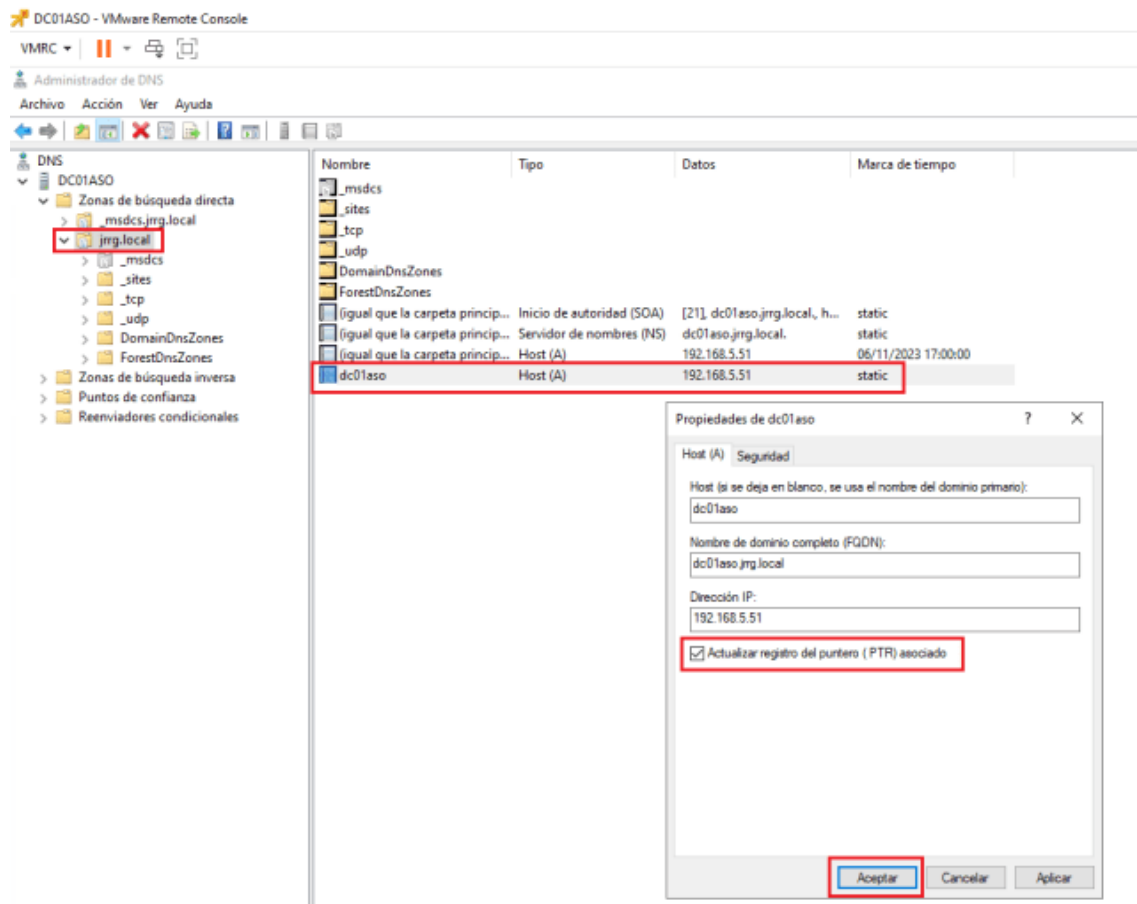
Tipo de búsqueda: Invertir

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.

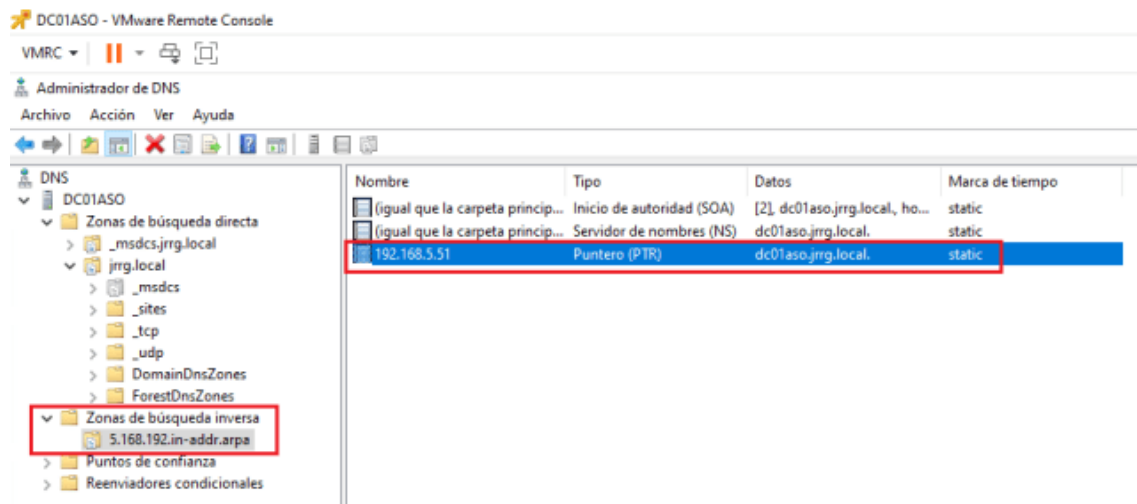
Para cerrar este asistente y crear la zona nueva, haga clic en Finalizar.

< Atrás **Finalizar** Cancelar

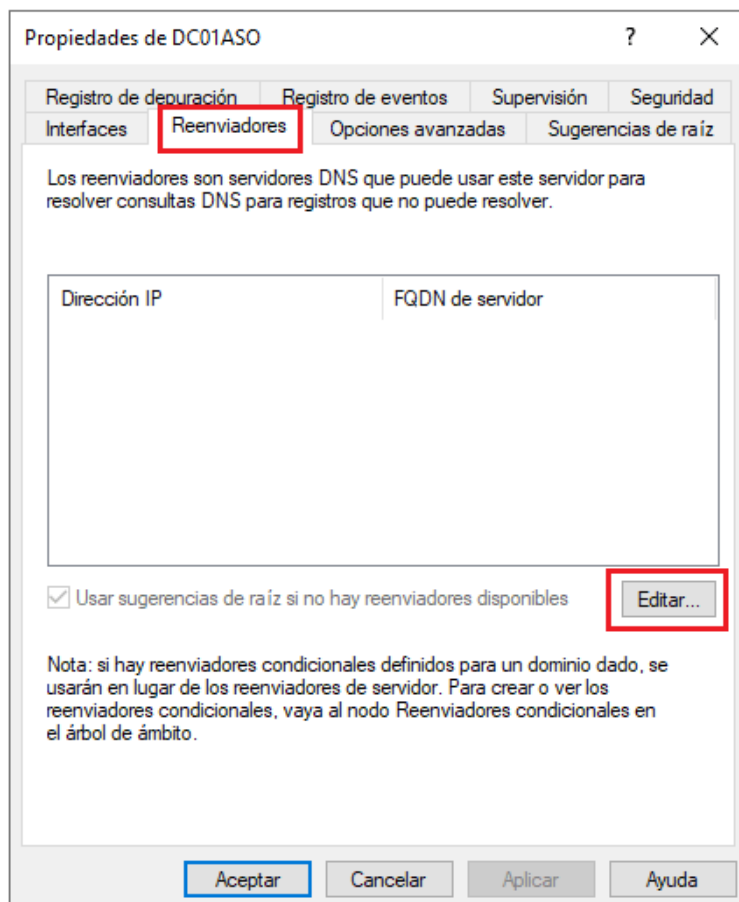
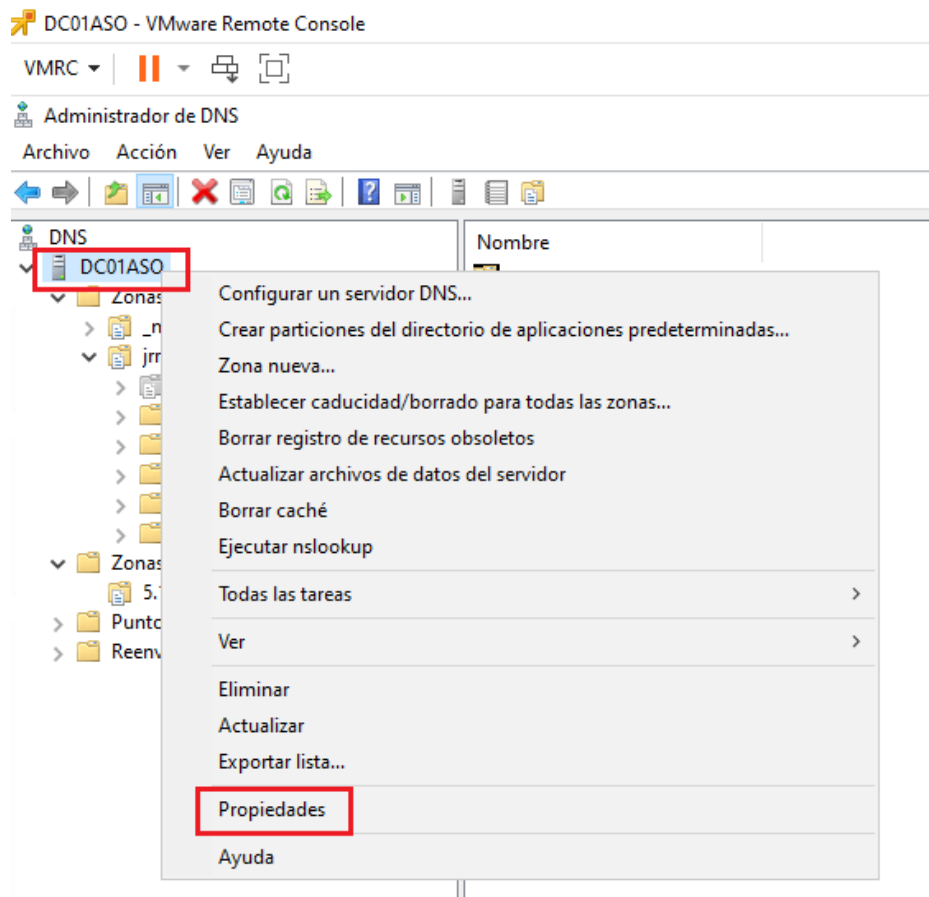
- Para verificar que la zona de resolución inversa está funcionando correctamente, sobre la zona de búsqueda directa y sobre las propiedades del registro tipo A de nuestro servidor controlador de dominio, marcamos el check PTR:

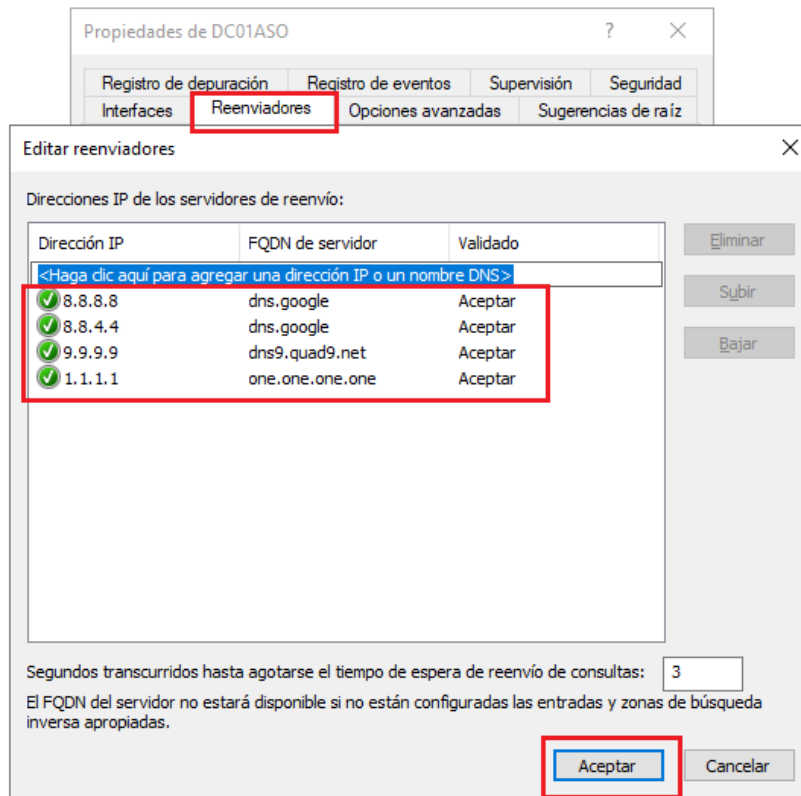


- Y como vemos en nuestra zona de búsqueda inversa se actualiza el registro:

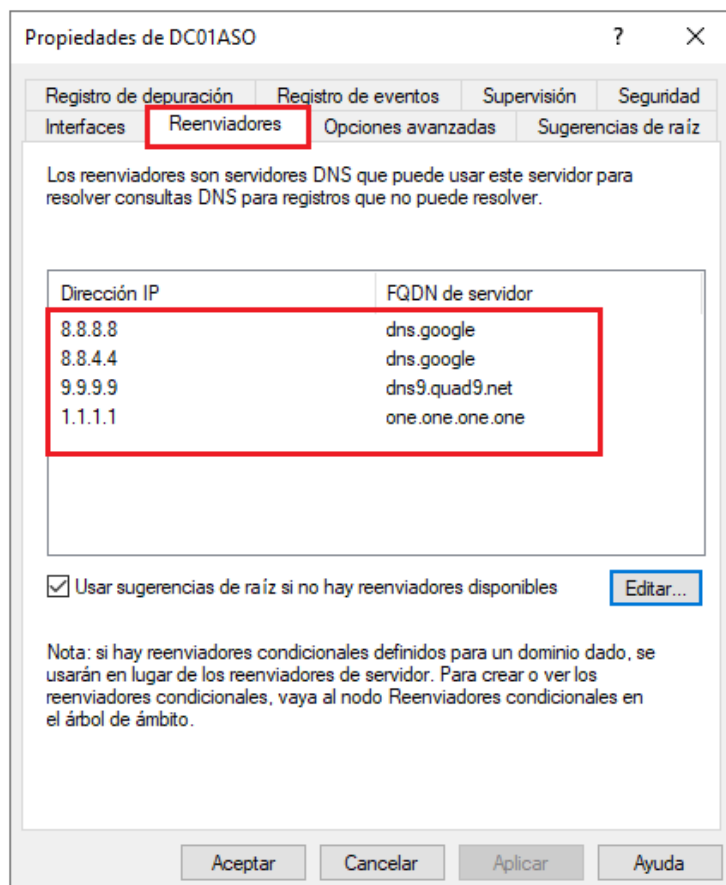


- Otra de las configuraciones que debemos realizar en nuestro DNS es agregar los reenviadores (pondremos los DNS públicos de google 8.8.8.8 y 8.8.4.4, el DNS público de IBM 9.9.9.9 especializado en bloquear malware) y el 1.1.1.1 para que el servidor DNS resuelva también dominios externos, para ello hacemos lo siguiente:

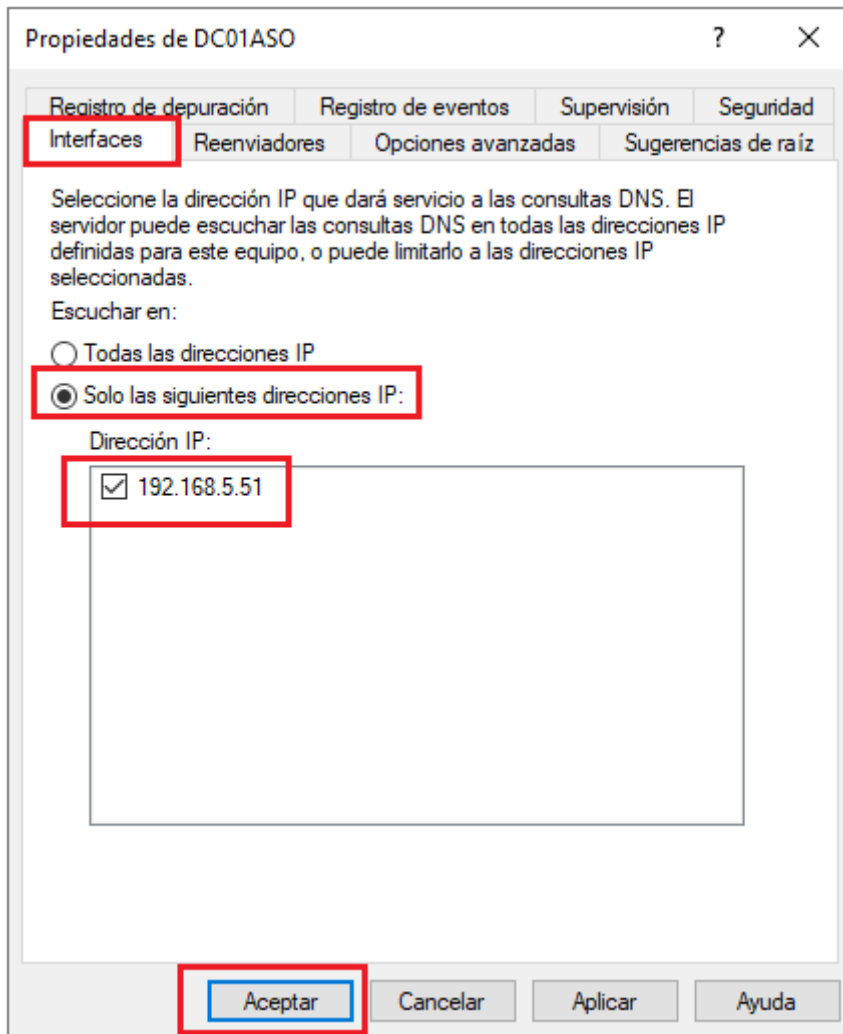




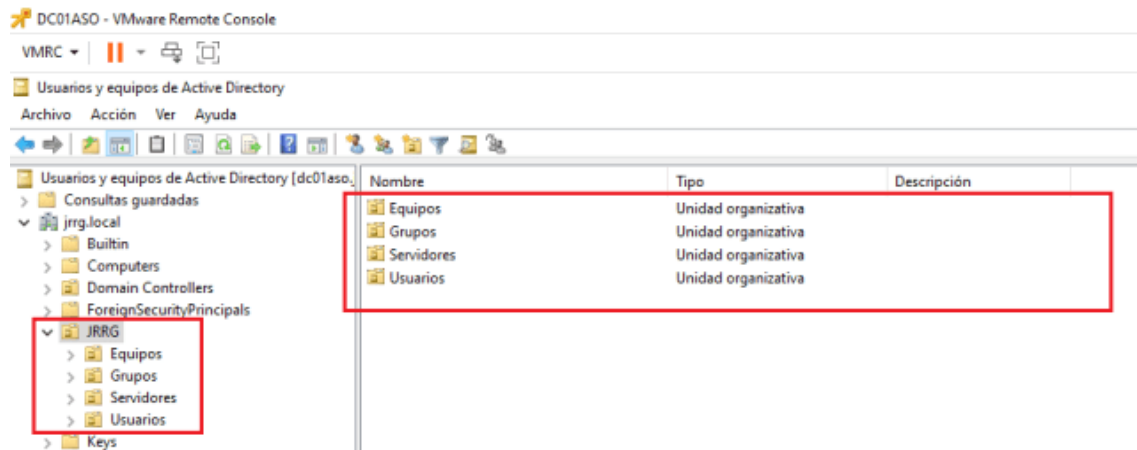
- Así quedarían configurados nuestros reenviadores:



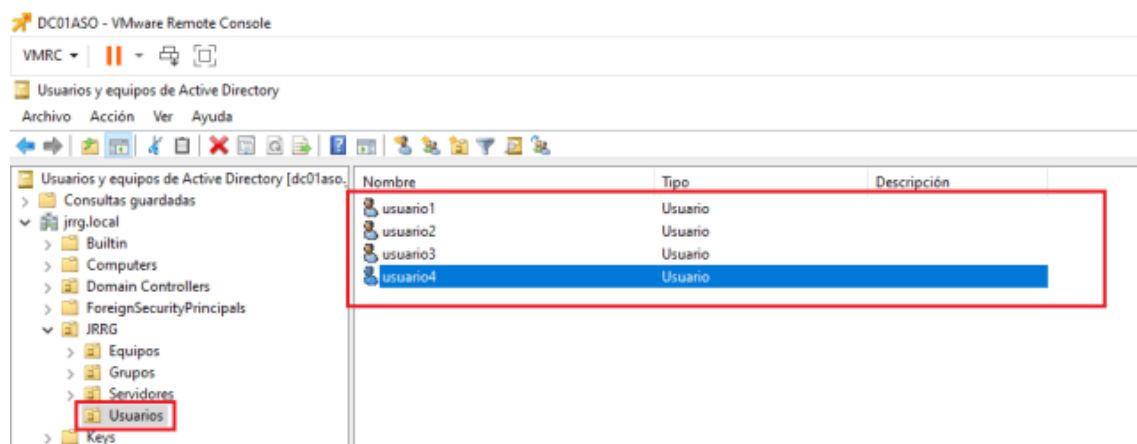
- Configuramos la dirección IP que dará servicio a las consultas DNS:



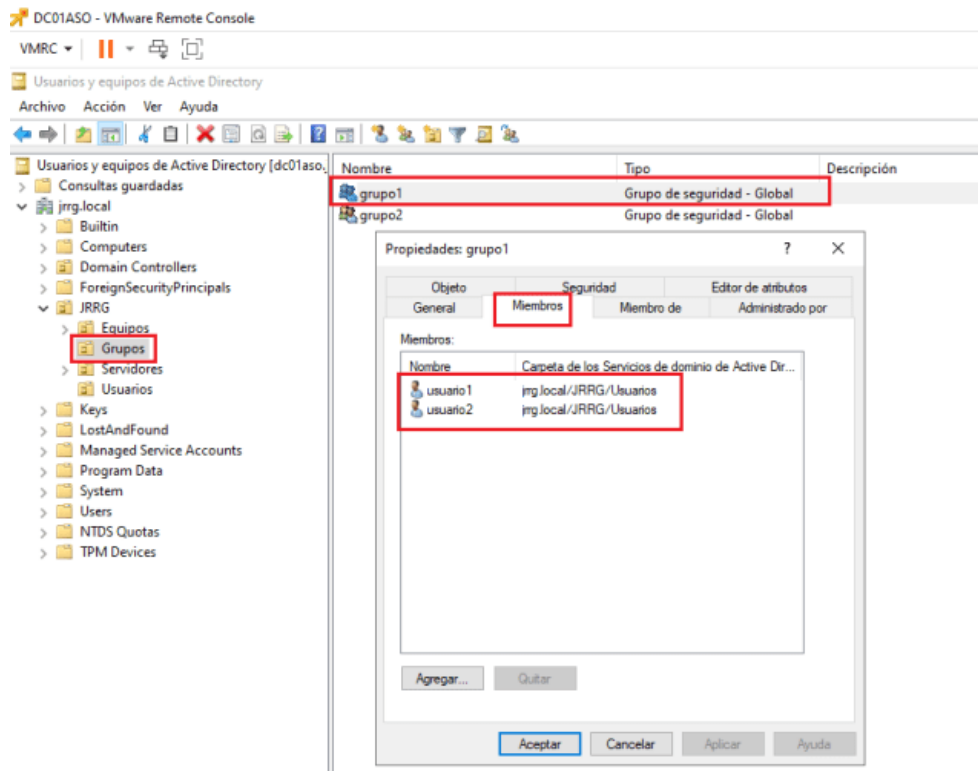
- Con todo esto, ya tendríamos nuestro controlador de dominio implementado en nuestra infraestructura, ya podríamos empezar a crear usuarios y a organizar el Active Directory.
- Ahora vamos a crear varias unidades organizativas, grupos y usuarios.
- Estas son las unidades organizativas que hemos creado:

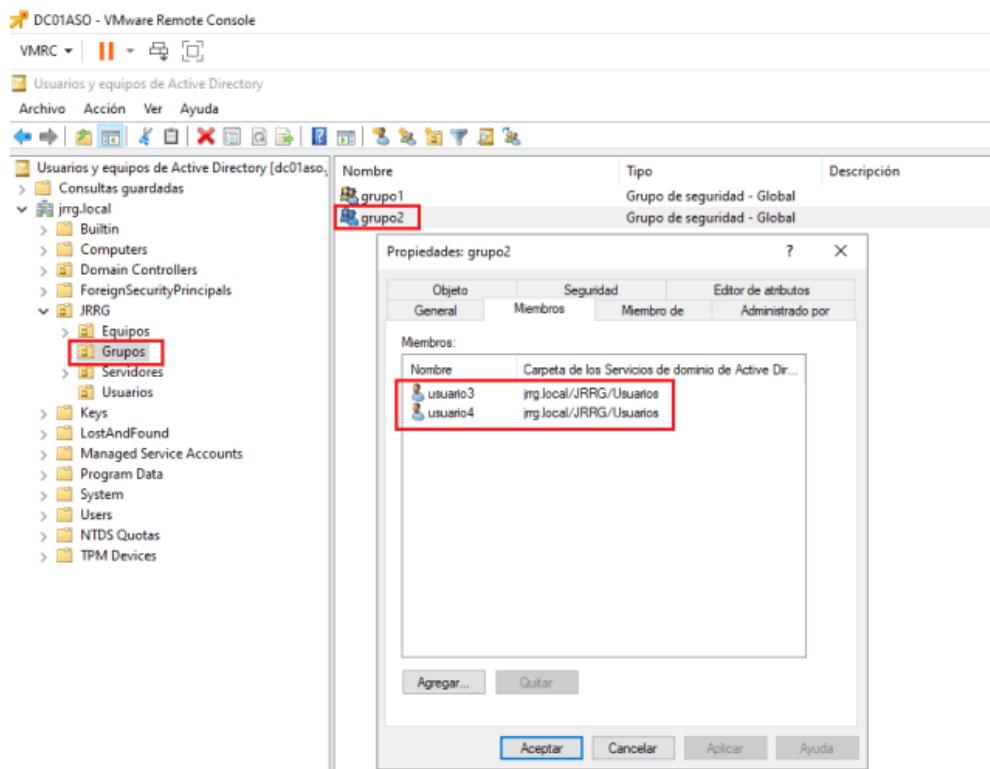


- Ahora vamos a crear varios usuarios:



- Crearemos dos grupos, cada uno de ellos con dos usuarios:





- Ahora vamos a crear una carpeta compartida en nuestro controlador de dominio llamada share, con permisos de escritura para los grupos creados, para el uso compartido avanzado le vamos a asignar control total a Todos, y luego filtraremos los permisos a los grupos creados con los permisos NTFS en Seguridad > Opciones avanzadas:

