

# Añadir otro controlador de dominio

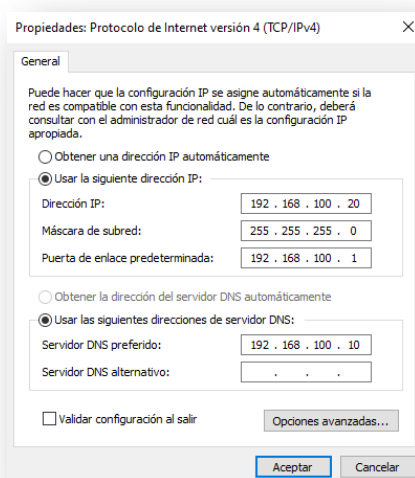
Un dominio con Active Directory puede funcionar perfectamente con un solo servidor, pero esta situación genera una total dependencia del funcionamiento de ese equipo y de la red a la que está conectada. Lo apropiado para tener tolerancia a fallos es tener un mínimo de 2 controladores de dominio. En función del número de usuarios y servicios prestados podríamos añadir más. Tal vez el factor más determinante sea la dispersión geográfica. Por ejemplo, una empresa con 300 usuarios podría ser gestionada con un único controlador de dominio, pero si la empresa tiene 3 sedes en Australia, España y México con 100 empleados cada una, lo mejor sería tener un controlador de dominio en cada ubicación.

Hay varias maneras de añadir un nuevo controlador de dominio. En esta guía veremos la que tiene una configuración más sencilla con los siguientes pasos:

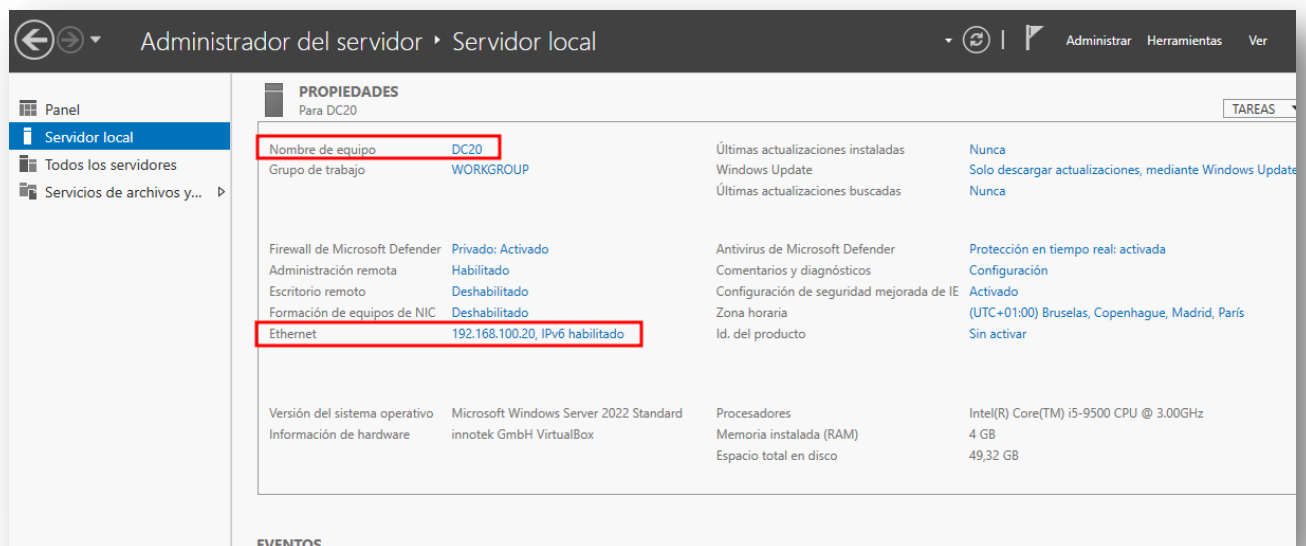
- Configuración inicial del equipo con nombre único e IP fija
- Añadir el equipo al dominio
- Promoción del equipo a controlador de dominio

## Configuración inicial

El primer paso consiste en preparar el equipo de manera que tenga un nombre único en el dominio, en mi caso lo llamaré "dc20". El siguiente paso requiere de configurar una IP fija para este servidor. Como ya hemos visto podríamos añadir una reserva en el DHCP o podemos configurar la IP a mano. En este caso voy a configurar la IP a mano porque no quiero que este controlador de dominio dependa del DHCP.



En este caso lo voy a configurar con la IP acabada en 20. Solo nos paramos en esta configuración para recordar que la puerta de enlace es la acabada en 1 porque aprovechamos la puerta de enlace que VirtualBox nos configura en la red NAT. También nos paramos a revisar la IP del DNS, aquí pondremos un DNS que sepa resolver los nombres del dominio. Si ponemos un DNS como 8.8.8.8 nunca llegaremos a "int.miempresa.es" y no nos podremos añadir al dominio.



Con estos pasos ya tenemos el equipo listo para ser añadido al dominio.

## Añadir equipo al dominio

En caso de estar utilizando una máquina clonada del controlador de dominio actual es necesario hacer un "sysprep" con la opción de "Generalizar" para cambiar el SID de la máquina:

```
C:\Windows\System32\Sysprep\sysprep.exe
```

Ya está documentado en otra guía como unir un equipo al dominio y en este caso, aunque el sistema operativo sea un servidor, el proceso es exactamente el mismo.

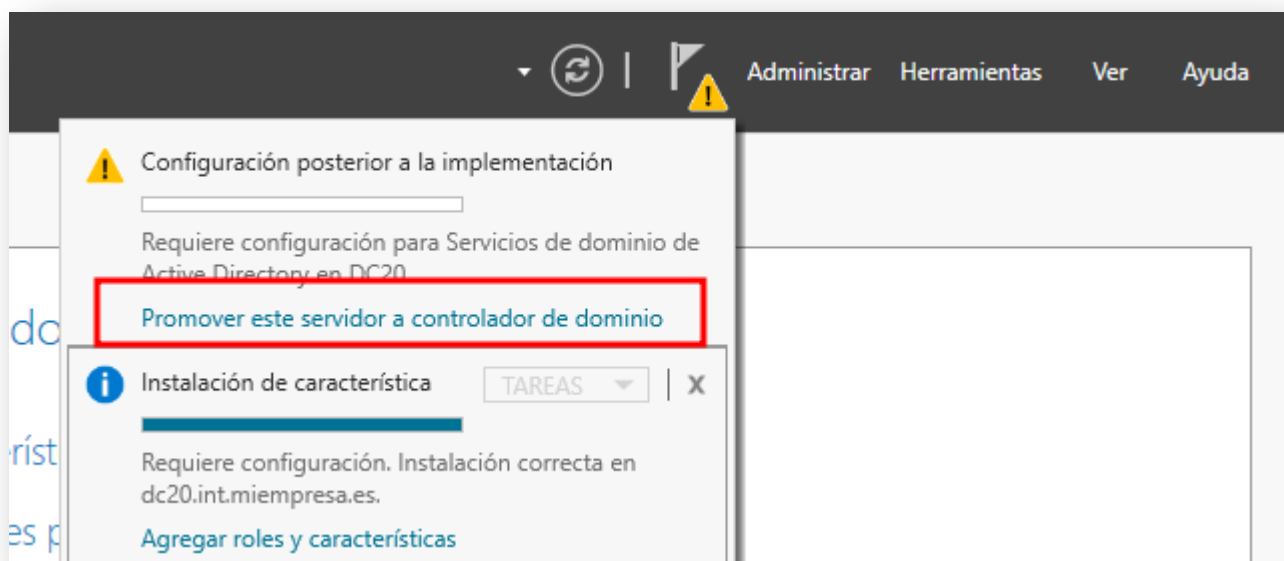
- Eliminamos la pertenencia al grupo de trabajo en favor del dominio y escribimos en la caja el nombre completo y exacto del dominio. En mi caso "int.miempresa.es". solo si el servidor DNS puede resolver esta dirección nos aparecerá el desafío.
- En el desafío tenemos que acreditararnos con un usuario del dominio que tenga permisos para añadir equipo al dominio. En este momento el único usuario con estos permisos es el administrador del dominio. Si nos acreditamos correctamente veremos una ventana en la que se confirma la unión al dominio y reiniciamos para que los cambios surjan efecto

## Promocionar a controlador de dominio

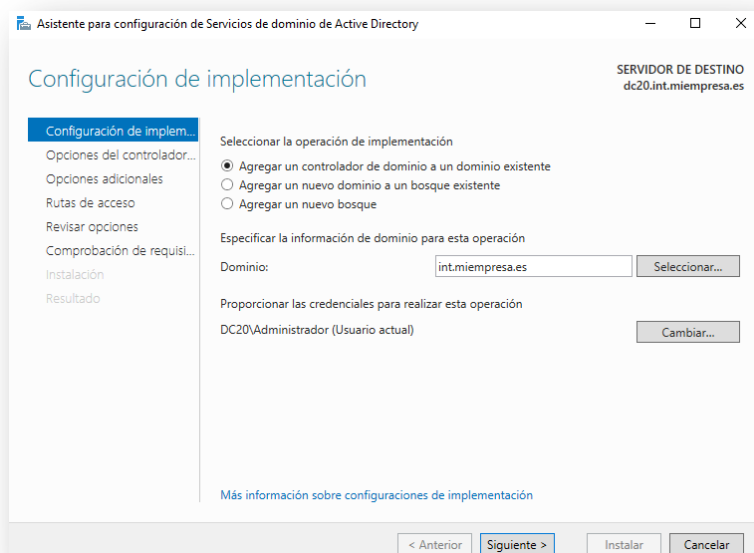
Una vez que ya estamos unidos al dominio podemos instalar Active Directory y promocionar a controlador de dominio. La parte positiva de haber añadido previamente este equipo al dominio es que muchas de las configuraciones ya estarán cubiertas.

De la misma manera que creamos el primer controlador del dominio, abrimos el "Asistente para agregar roles y características" y marcamos "Servicios de dominio de Active Directory" con las características por defecto que nos indique.

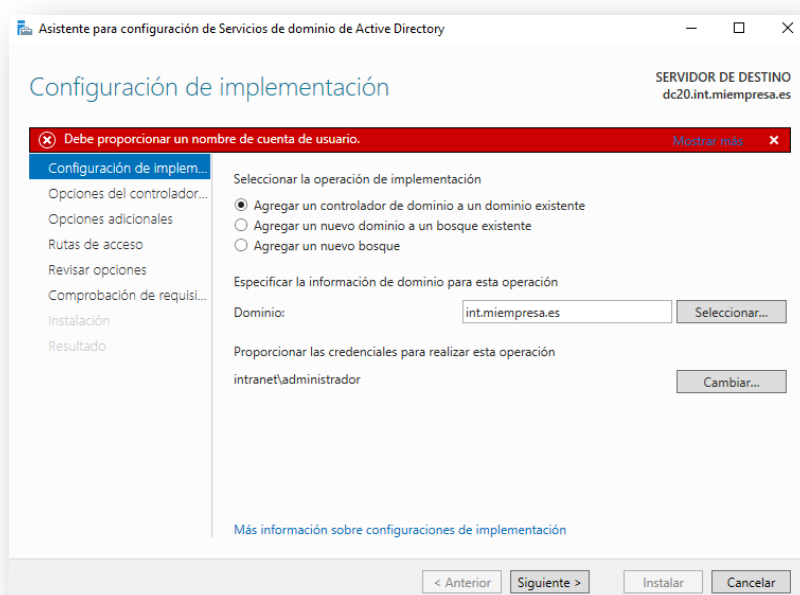
Con este paso se habrá instalado el software, pero es necesario promocionar el equipo para configurarlo como controlador de dominio. Este paso es el que cambia mínimamente respecto a la configuración del primer controlador. Pulsaremos sobre "Promover este servidor a controlador de dominio" y, a continuación nos aparecerá el asistente.



En la primera ventana nos pregunta qué tipo de implementación se va a hacer. En este caso lo que queremos es "Agregar un controlador de dominio a un dominio existente". La ventaja de haber añadido el equipo al dominio previamente es que nos ha cubierto los datos automáticamente.



Solamente tendremos que modificar las credenciales para realizar la operación. Ahora mismo está puesto el administrador local del equipo pero para añadir un segundo controlador tenemos que acreditarnos mediante un administrador del dominio. Para ello pulsamos en "Cambiar" y nos acreditamos con la cuenta administradora del dominio.

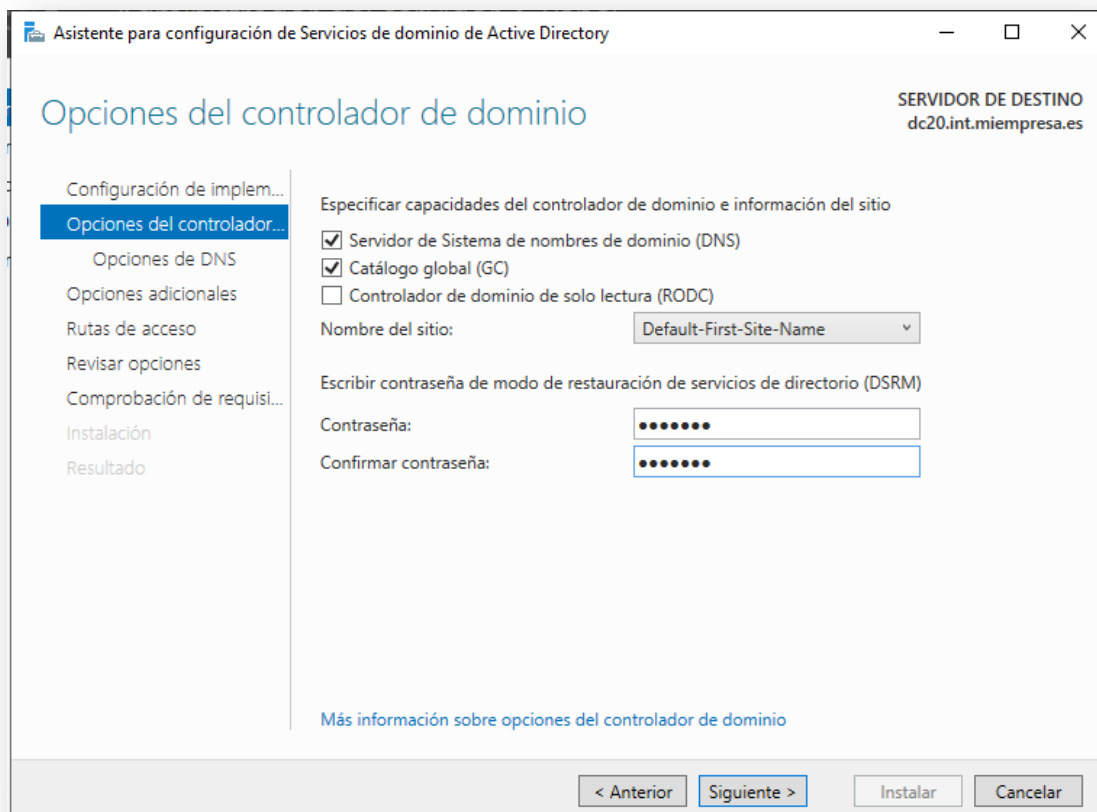


En la siguiente ventana nos preguntará si queremos replicar el DNS y si queremos que este controlador guarde el "Catálogo global", a ambas diremos que sí. También escribiremos la contraseña que queramos para la posible restauración en este equipo.

El servidor DNS debe ser marcado por defecto. Esto creará un segundo servidor DNS que estará perfectamente integrado con el primero. Active Directory controla el DNS en una forma especial. Todos los DNS estarán sincronizados automáticamente y proporcionarán alta disponibilidad con distribución de carga. Algo que llamará la atención es que todos serán autoritativos y será su propio SOA. Solo no marcaremos esta opción si ya tenemos un DNS bien configurado con otras herramientas como BIND.

El "Catálogo Global" es una copia resumen de los objetos del bosque con los atributos más utilizados. El objetivo es que un usuario se pueda acreditar entre dominios de un mismo bosque. Si nuestra empresa tiene varias sedes y hay mucho movimiento de personal entre ellas, tener marcada esta opción acelera mucho las autenticaciones de usuarios. En general lo tendremos siempre activado a no ser que este controlador tenga fuertes restricciones o limitaciones en la conexión a internet.

La opción de "Controlador de dominio de solo lectura" solo debe marcarse en escenarios donde la seguridad del servidor pueda verse comprometida ya que no almacena contraseñas ni puede hacer cambios en el dominio.

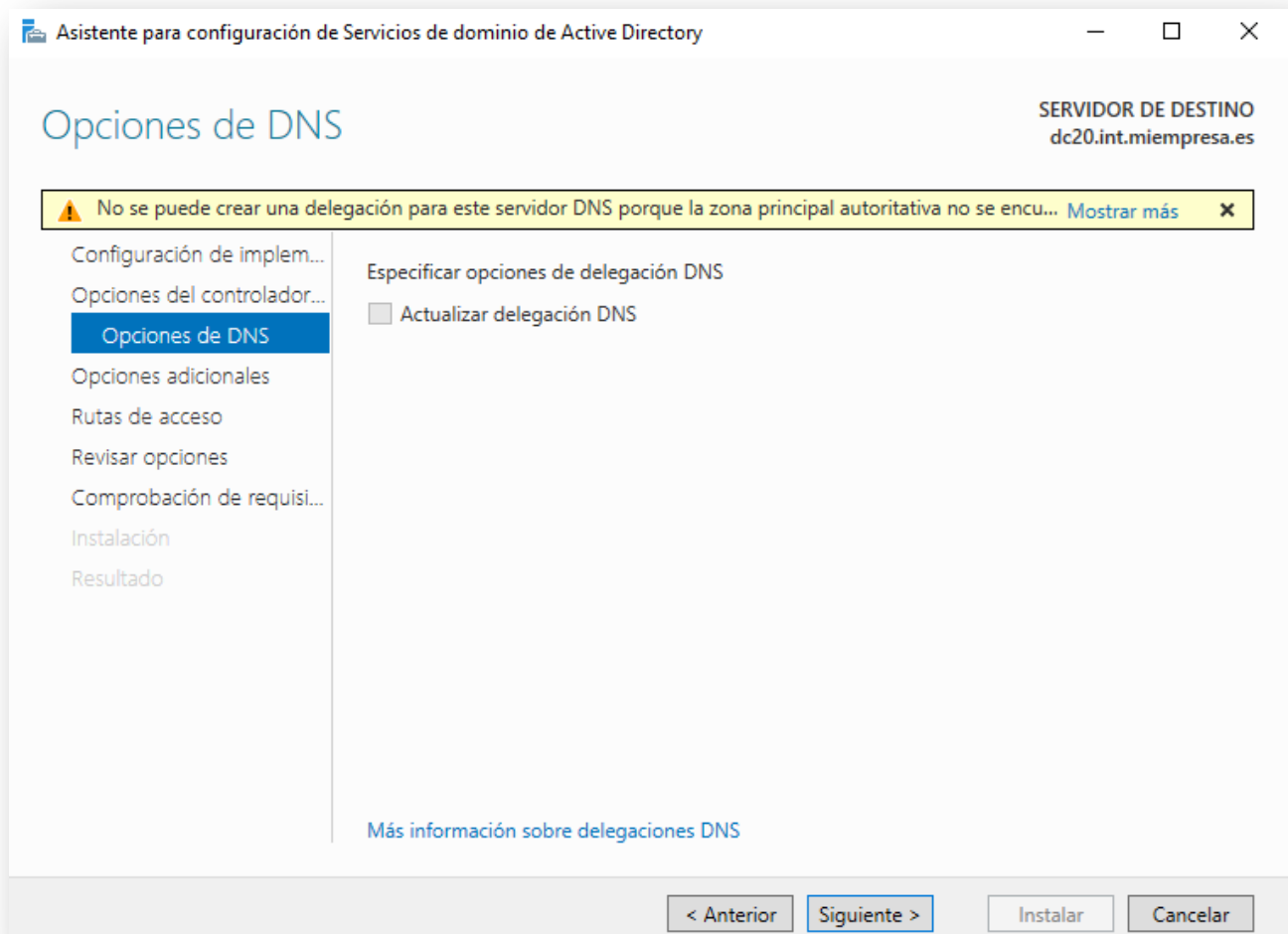




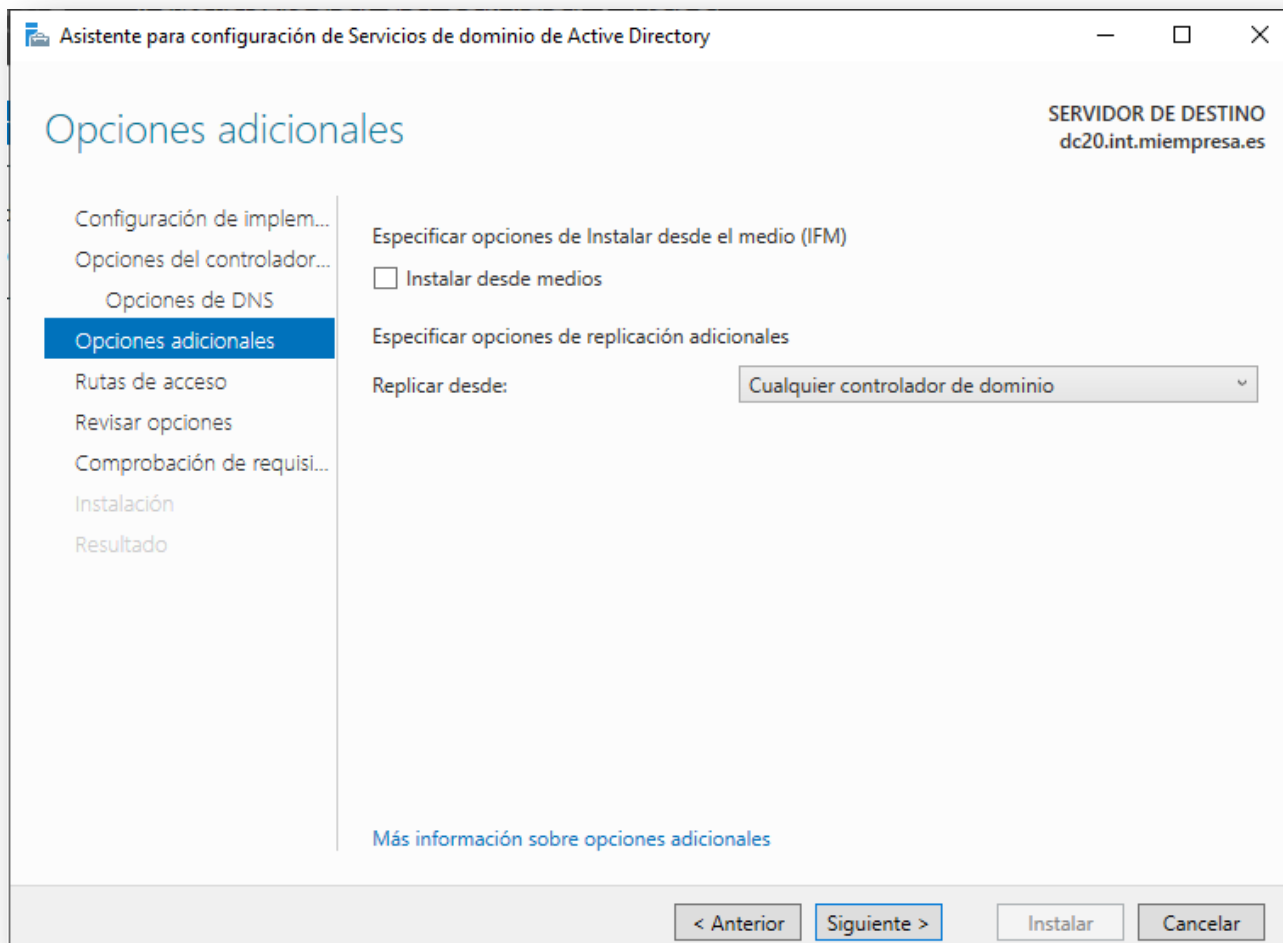
La siguiente ventana trata sobre el DNS y la vamos a dejar tal cual.

La delegación DNS la marcaríamos en caso de querer gestionar un subdominio. En nuestro caso estamos añadiendo un segundo controlador de dominio al mismo dominio así que no hay que delegar nada, simplemente replicar el que ya existe.

Marcar la opción de delegación sería para crear un DNS que resuelva solo un subdominio de "int.miempresa.es", por ejemplo, "ventas.int.miempresa.es". Esta opción crearía un registro NS en el DNS principal haciendo que todas las consultas a "ventas.int.miempresa.es" apunten a este nuevo servidor.



La siguiente ventana nos pregunta cómo vamos a replicar/copiar los datos del dominio a este nuevo controlador. Podríamos volcarlos desde una imagen de un repositorio o bien seleccionar algún servidor en concreto (o cualquiera). Lo dejaremos como está para que copie todo el catálogo desde nuestro único controlador activo.



**Asistente para configuración de Servicios de dominio de Active Directory**

**Opciones adicionales**

SERVIDOR DE DESTINO  
dc20.int.miempresa.es

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

Especificar opciones de Instalar desde el medio (IFM)  
☐ Instalar desde medios

Especificar opciones de replicación adicionales  
Replicar desde: Cualquier controlador de dominio

[Más información sobre opciones adicionales](#)

< Anterior **Siguiente >** Instalar Cancelar

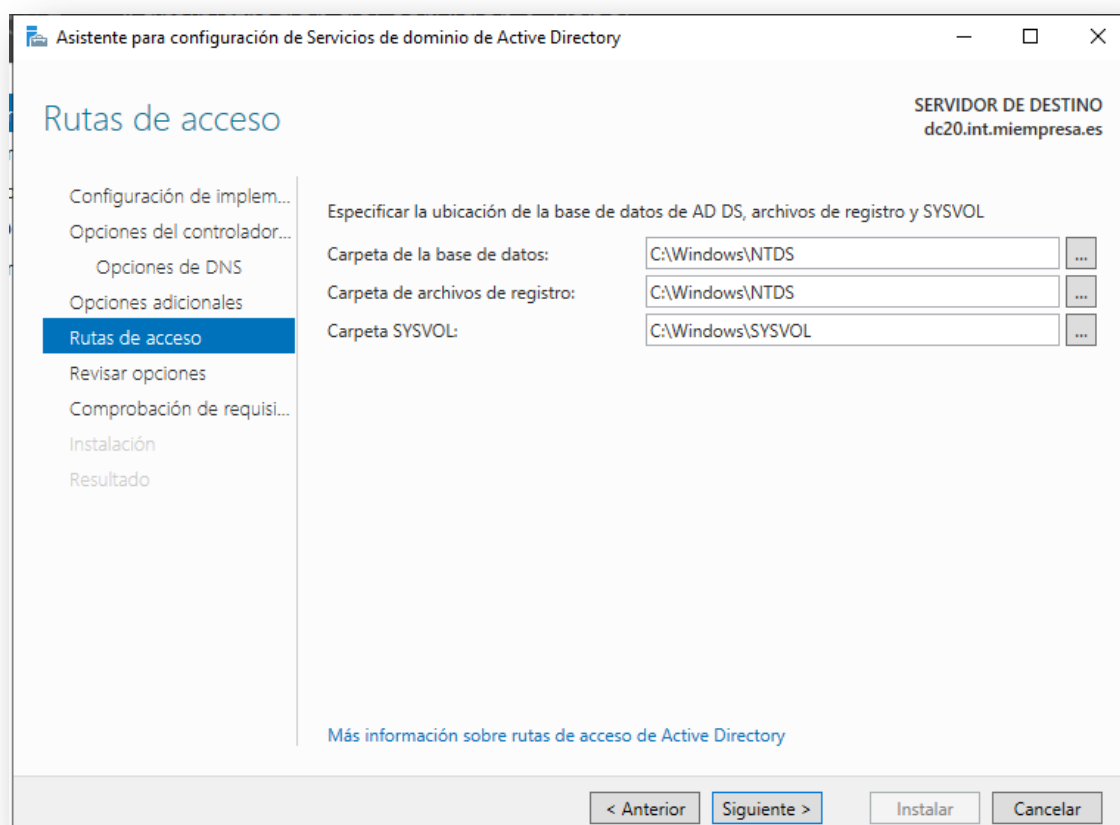
En la siguiente ventana nos pregunta por la ubicación de las carpetas que usa el controlador para guardar la información del dominio. La dejamos como está.

La carpeta de la base de datos almacena el esquema de Active Directory del bosque y el dominio. Además también se guardan los objetos de dominio como los usuarios, grupos y unidades organizativas.

La carpeta de archivos de registro guarda principalmente archivos de registro de transacciones y logs.

La carpeta SYSVOL es una carpeta compartida donde se almacenan las GPOs, scripts y otros archivos compartidos.

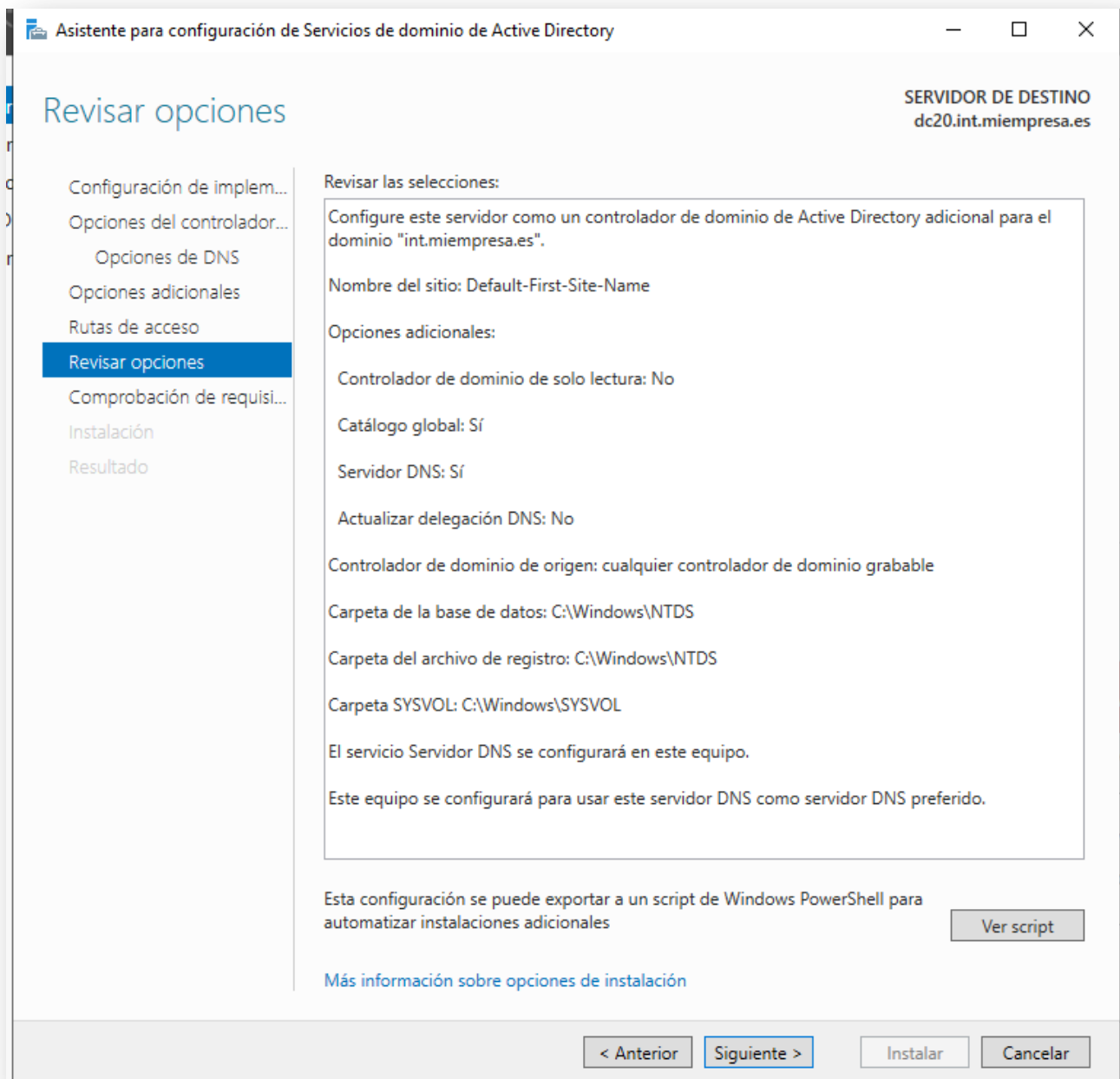
La ubicación física de estas carpetas debe ser bien planificada en “producción”. Por ejemplo, la base de datos y los archivos de registro son complementarias y deberían estar en máquinas distintas para, en caso de fallo, poder recuperar el estado anterior. Hay que tener en cuenta que la base de datos puede crecer hasta los varios gigabytes, no se compacta aunque borremos objetos como usuarios o GPOs. Los archivos de registro ocupan bastante menos, unos cientos de megas pero se escriben constantemente





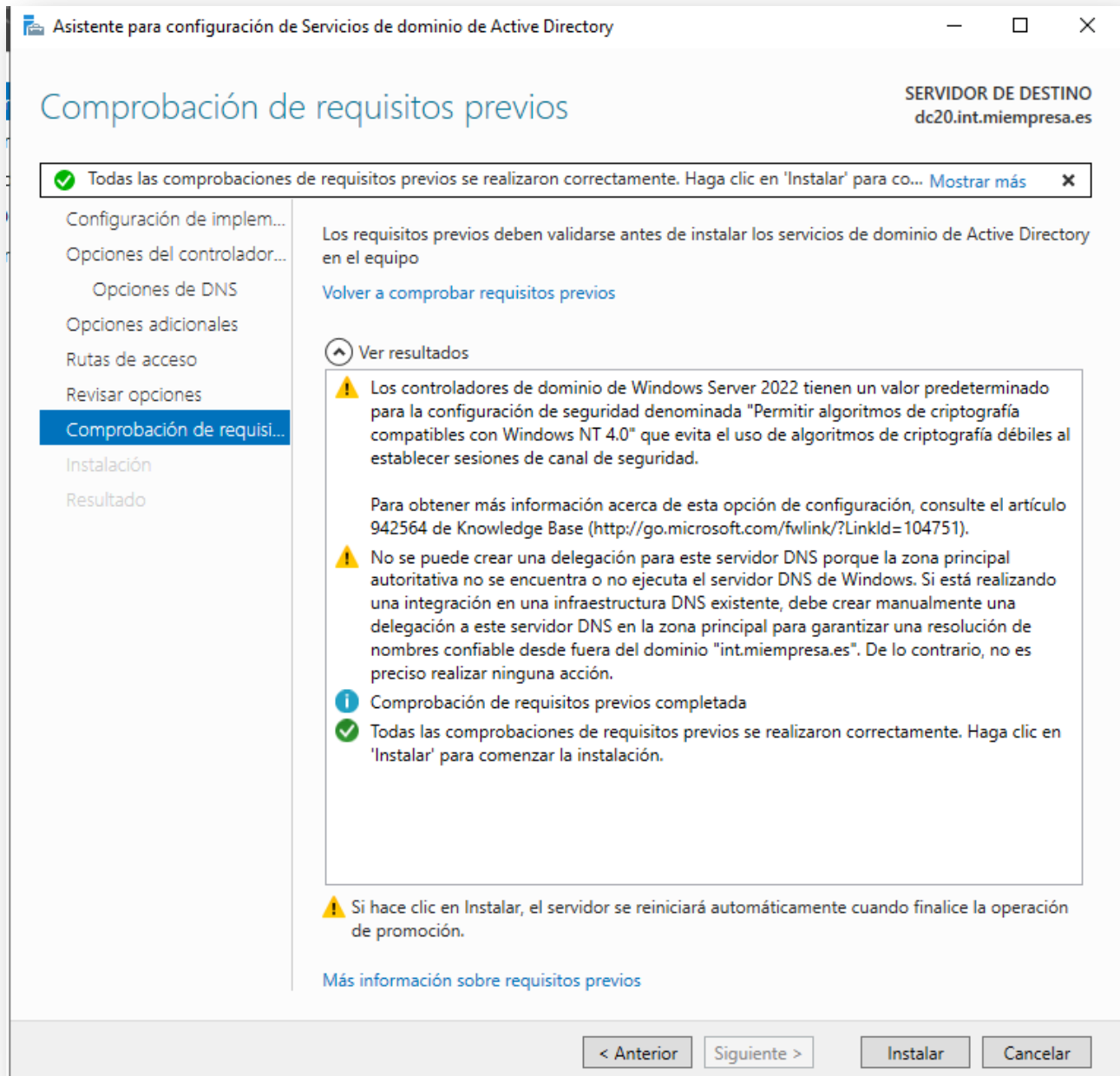


Con esto llegamos a la ventana final donde aparece un resumen.



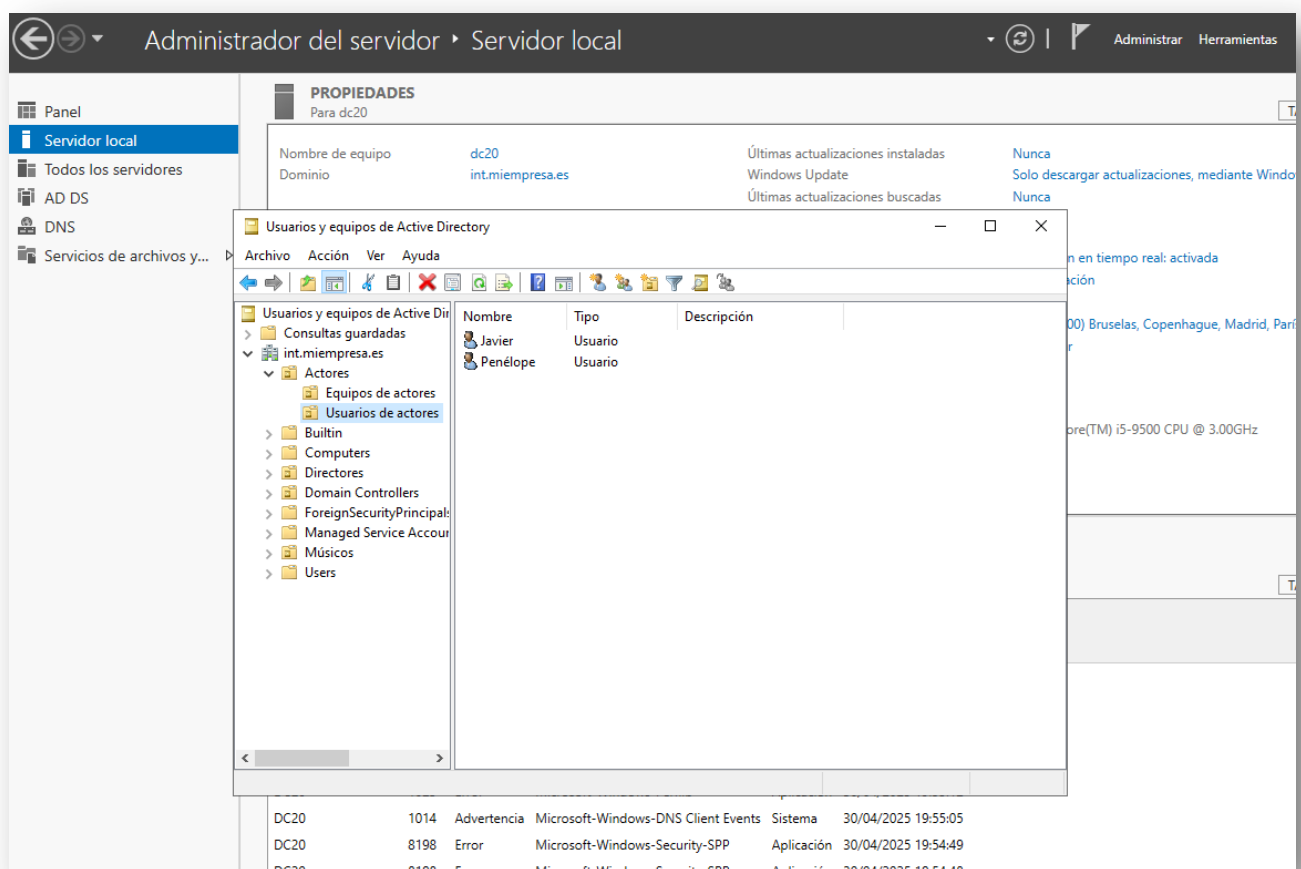


El último paso consiste en confirmar que el equipo es apto para funcionar como controlador de dominio y ya por fin, instalar.



Para finalizar tendremos un reinicio. Una vez que arranquemos sesión en el nuevo controlador podremos comprobar que tanto los usuarios, los equipos y todas las GPOs se encuentran ya replicadas en el nuevo controlador.

En la siguiente captura vemos como al abrir la herramienta de “Usuarios y equipos de Active Directory” del nuevo controlador de dominio podemos ver la estructura que definimos previamente en el primer controlador de dominio. A partir de este momento, el esquema estará replicado en ambos controladores de manera que los cambios hechos en uno se reflejarán inmediatamente en el otro.



Todos los demás servicios vinculados al dominio también ser replicarán. En nuestro caso el DNS también está vinculado al dominio por lo que será Active Directory el encargado de replicarlo entre los controladores del dominio.