



Actividad 4.3 **Implementación de Active Directory**

Duración estimada: 60 minutos

Objetivos

Esta actividad de laboratorio se concentrará en su capacidad para realizar las siguientes tareas:

- Configurar Active Directory en Windows 2000 Server
- Comprobar el funcionamiento del servicio de directorios

Recursos

Serán necesarios los siguientes recursos para desarrollar la clase:

- PC con Windows 2000 Server para actuar como controlador de dominio
- PC con Windows 2000 Professional para actuar como cliente

Información adicional

En una red de Microsoft Windows 2000, el servicio de directorio Active Directory proporciona la estructura y las funciones para organizar, administrar y controlar el acceso a los recursos de red.

Para implementar y administrar una red de Windows 2000, deberá comprender el propósito y la estructura de Active Directory.

Active Directory proporciona también la capacidad de administrar centralmente la red de Windows 2000 Server. Esta capacidad significa que puede almacenar centralmente información acerca de la empresa, por ejemplo, información de usuarios, grupos e impresoras, y que los administradores pueden administrar la red desde una sola ubicación.

Active Directory admite la delegación del control administrativo sobre los objetos de él mismo. Esta delegación permite que los administradores asignen a un grupo determinado de administradores, permisos administrativos específicos para objetos, como cuentas de usuario o de grupo.

Active Directory es el servicio de directorio de una red de Windows 2000, mientras que un servicio de directorio es aquel que almacena información acerca de los recursos de la red y permite que los mismos resulten accesibles a los usuarios y a las aplicaciones. Los servicios de directorio proporcionan una manera coherente de nombrar, describir, localizar, tener acceso, administrar y asegurar la información relativa a los recursos de red.



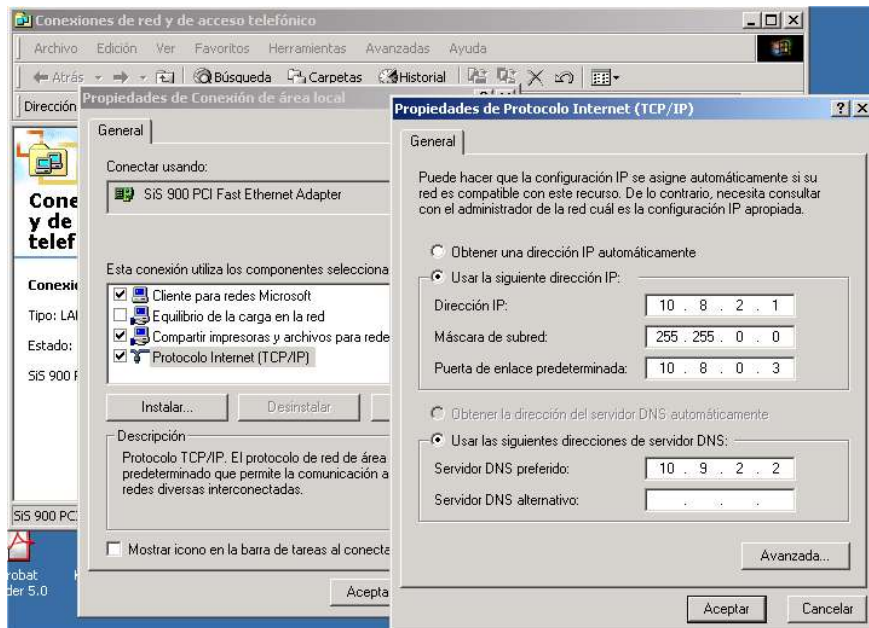
Desarrollo

Paso 1 Configuraciones previas

Antes de comenzar la configuración de Active Directory, es necesario realizar un conjunto de configuraciones previas en el servidor Windows 2000.

Direccionamiento estático

El primer paso es configurar el servidor con un esquema de direccionamiento estático.

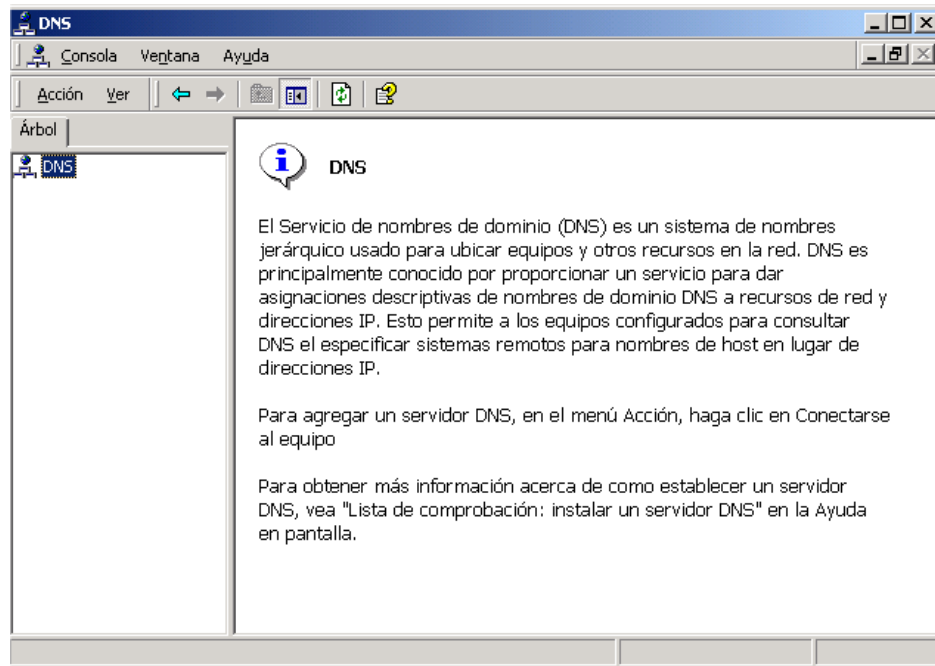


Configure los servidores según el siguiente esquema de direccionamiento.

Servidor	Dirección IP	Máscara	Gateway	DNS
Grupo1	10.2.110.1	255.255.0.0	10.2.1.50	10.1.1.20
Grupo2	10.2.120.1	255.255.0.0	10.2.1.50	10.1.1.20
Grupo3	10.2.130.1	255.255.0.0	10.2.1.50	10.1.1.20
Grupo4	10.2.140.1	255.255.0.0	10.2.1.50	10.1.1.20
Grupo5	10.2.150.1	255.255.0.0	10.2.1.50	10.1.1.20

Configuración del servicio DNS

Abra el administrador de nombres de dominio. Haga clic en Inicio => Programas => Herramientas Administrativas => DNS.

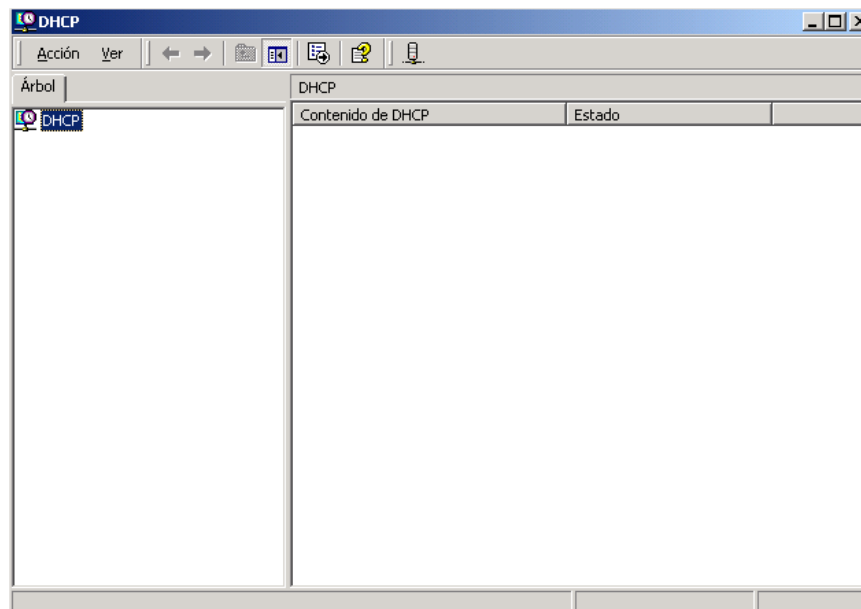


Elimine el o los servidor/es DNS que se encuentren listados en el árbol de consola. Cierre el administrador de DNS.

Configurar el servidor DHCP

Abra la consola de administración de DHCP. Vaya a Inicio => Programas => Herramientas Administrativas = DHCP.

Elimine el servidor DHCP listado en el árbol de DHCP.

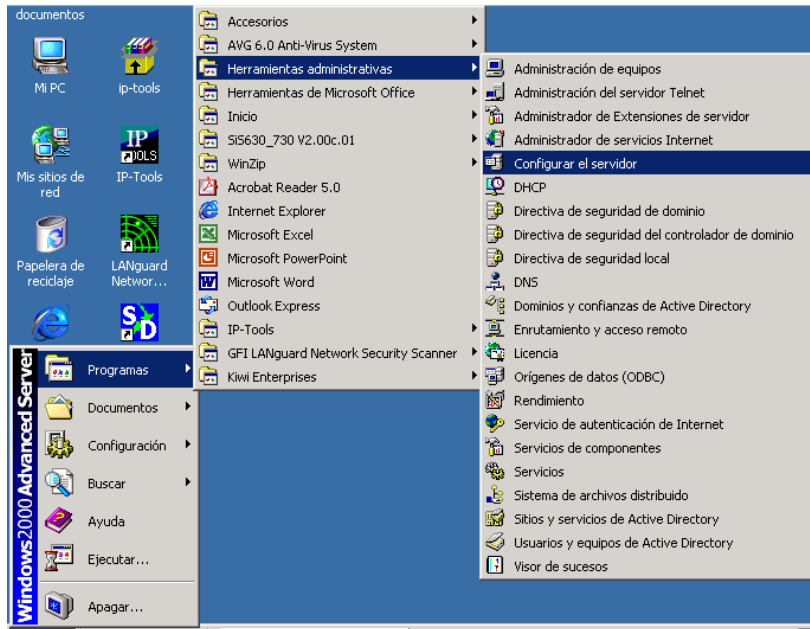




Paso 2 Instalación del controlador de dominio de Active Directory

Para instalar el Primer controlador deberemos seguir los siguientes pasos.

Iniciar la Herramienta Configuración del Servidor desde el menú de Herramientas Administrativas.

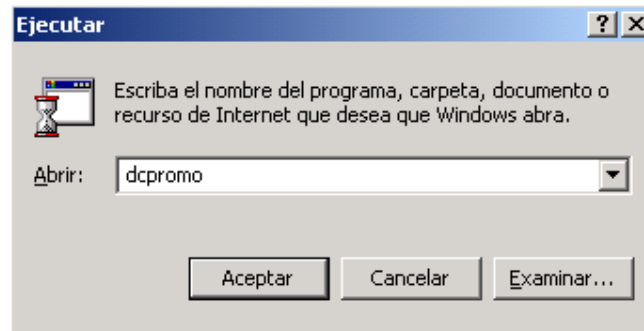


En la ventana que se abre, en el menú de la derecha hay que elegir la opción Active Directory.



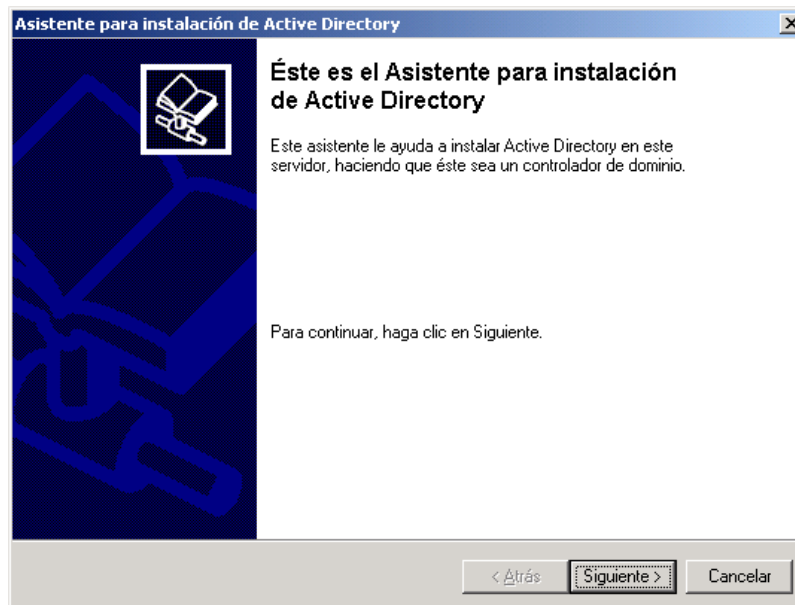


También puede iniciar el asistente directamente ejecutando el archivo ejecutable Dcpromo.exe desde el cuadro de dialogo Ejecutar.



Los usuarios también pueden ejecutar el archivo desde el símbolo del sistema después de iniciar sesión por medio de la cuenta de administrador local. Dcpromo.exe se encuentra en la carpeta %SystemRoot%\System32, lo que permite ejecutarlos desde cualquier carpeta sin especificar una ruta de acceso.

Lo primero que se presenta es la pantalla de bienvenida al asistente de Active Directory.



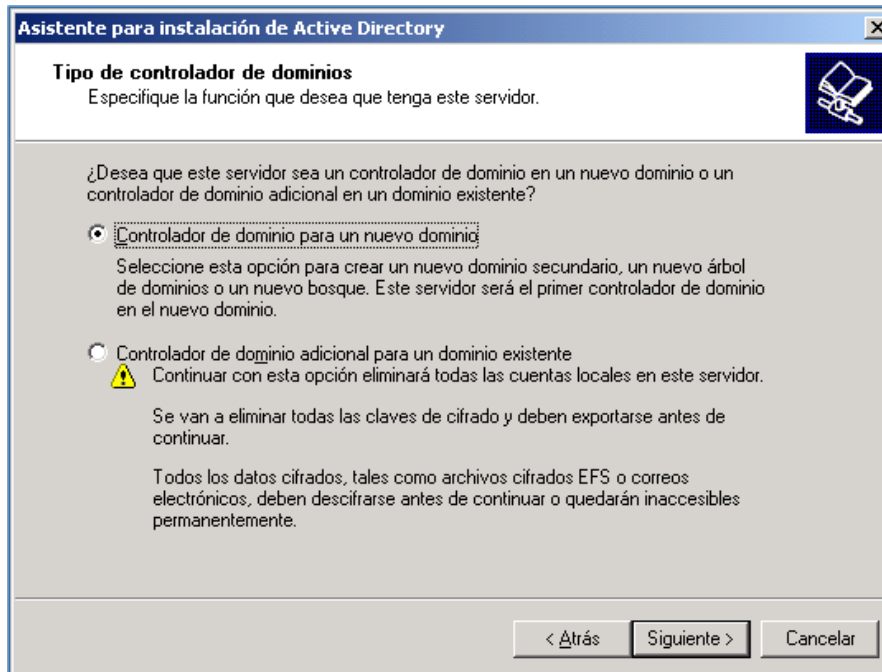
Haga clic en Siguiente.

A continuación se presenta la ventana que permite elegir el Tipo de Controlador de Dominios. El Asistente para instalación pregunta sobre la acción que se va a realizar, basándose en el estado actual de Active Directory en el sistema. Si el servidor ya es un controlador de dominio, el asistente solo proporciona la opción de degradar el sistema de nuevo a servidor independiente o miembro.



En un equipo que no es un controlador de dominio, el asistente muestra la pantalla Tipo de controlador de dominios, la cual pide que se seleccione una de las siguientes opciones:

- Controlador de dominio para un nuevo dominio: Instala Active Directory en el servidor y lo designa como el primer controlador de dominio de un nuevo dominio.
- Controlador de dominio adicional para un dominio existente: Instala Active Directory en el servidor y replica la información del directorio desde un dominio existente.



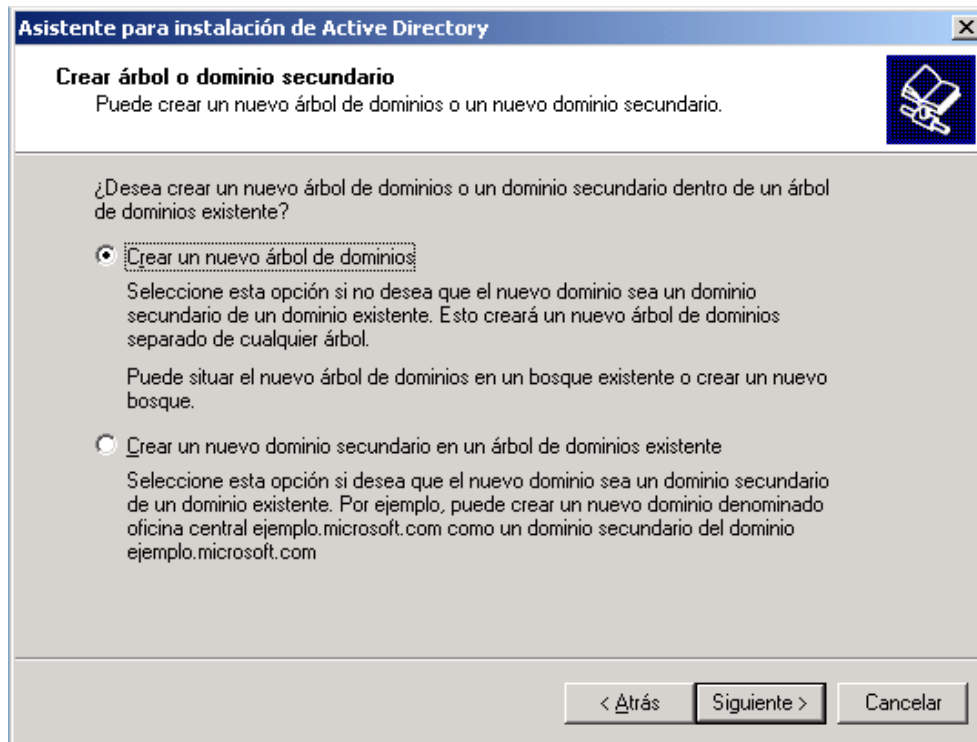
Para instalar el primer servidor Active Directory en la red, se selecciona la opción Controlador de dominio para un nuevo dominio. Esto hace que el asistente instale los archivos de soporte de Active Directory, cree el nuevo dominio y lo registre en el DNS . Haga clic en Siguiente.

En la siguiente ventana, el asistente presenta la pantalla para Crear árbol o dominio secundario. Debemos elegir el tipo de dominio que queremos configurar de las dos opciones que se presentan en el siguiente cuadro.

- Crear un nuevo árbol de dominios: Configura el nuevo controlador de dominio para que aloje el primer dominio de un nuevo árbol.
- Crear un nuevo dominio secundario en un árbol de dominios existente: Configura el nuevo controlador de dominio para que aloje un hijo de un dominio de un árbol que ya existe.

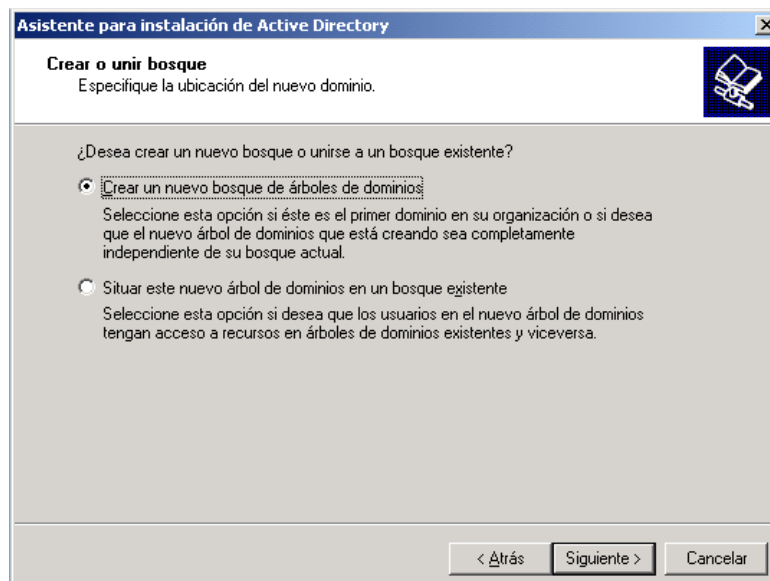
En nuestro caso deberemos elegir Crear un nuevo árbol de dominios.

Haga clic en Siguiente.



En la siguiente ventana el asistente consulta si Crear o unir bosque, que permite especificar una de las siguientes opciones:

- Crear un nuevo bosque de árboles de dominios: Configura el controlador de dominio para que sea la raíz de un nuevo bosque de árboles.
- Situar este nuevo árbol de dominios en un bosque existente: Configura el controlador de dominio para que aloje el primer dominio de un nuevo árbol en un bosque que ya contiene uno o más árboles.





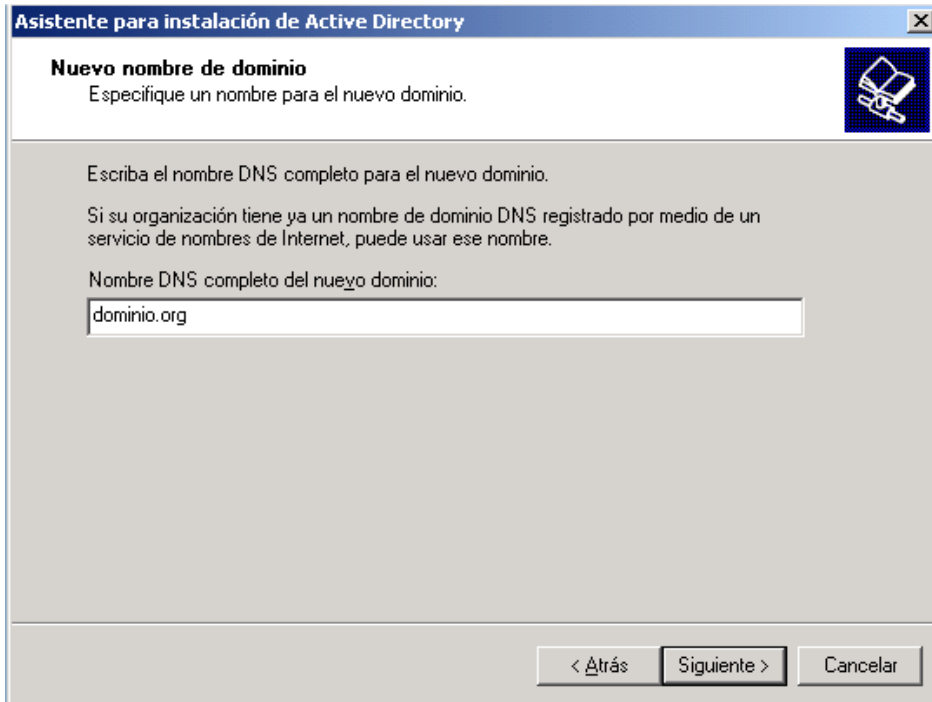
En este caso hay que seleccionar Crear un nuevo bosque de árboles de dominios, porque el primer controlador de dominio Windows 2000 de la red será siempre un nuevo dominio, en un nuevo árbol, en un nuevo bosque. A medida que se instalen controladores de dominio adicionales, se pueden utilizar estas mismas opciones para crear otros bosques nuevos o para poblar el bosque existente con árboles y dominios adicionales.

Haga clic en Siguiente.

A continuación se presenta la ventana Nombre de nuevo Dominio. Para identificar el controlador de dominio en la red se debe especificar un nombre DNS válido para el dominio que se está creando.

Este nombre no tiene por qué ser el mismo que el del dominio que utiliza la empresa para su presencia en Internet (aunque puede serlo). El nombre tampoco tiene que estar registrado en el Centro de información de redes de Internet (InterNIC, Internet Network information), la organización responsable de mantener el registro de los nombres DNS en los dominios de nivel superior com, net, org y edu. Sin embargo, el uso de un nombre de dominio registrado es una buena idea si los usuarios de la red van a acceder a los recursos de Internet al mismo tiempo que a los recursos de red locales, o si los usuarios externos a la organización accederán a los recursos de red locales vía Internet.

Cuando los usuarios acceden a los recursos de Internet al mismo tiempo que a los recursos de la red Windows 2000, existe la posibilidad de que un nombre de dominio no registrado entre en conflicto con un dominio de Internet registrado que utilice el mismo nombre. Cuando los usuarios de Internet tengan permiso para acceder a los recursos de la red utilizando protocolos estándar de la capa de aplicación como HTTP y FTP, puede surgir alguna confusión si los usuarios internos y los externos deben utilizar diferentes nombres de dominio.



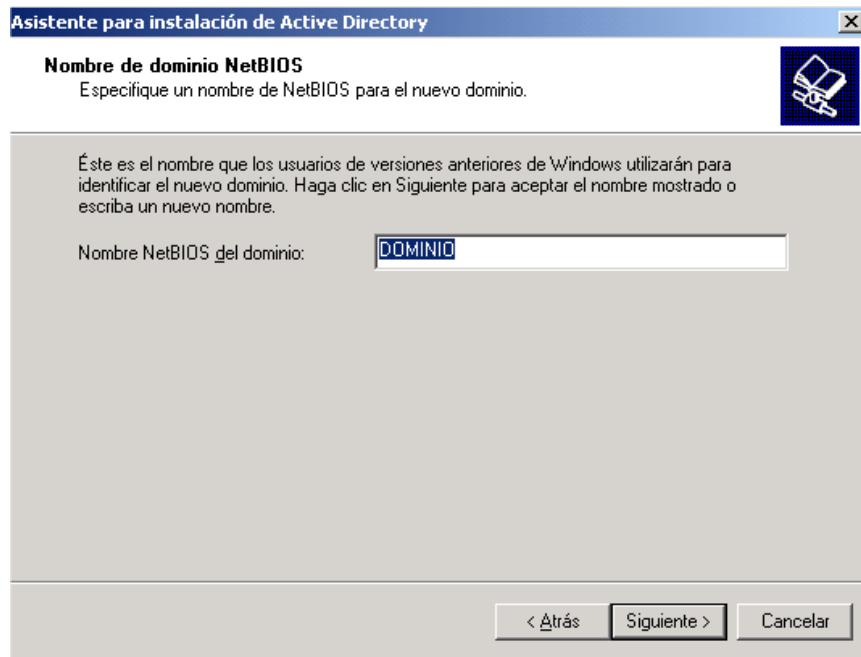
Configure el siguiente nombre de dominio según el servidor que esté configurando.

Servidor	Nombre DNS
Grupo1	domain1.org
Grupo2	domain3.org
Grupo3	domain5.org
Grupo4	domain7.org
Grupo5	domain9.org

Haga clic en Siguiete.

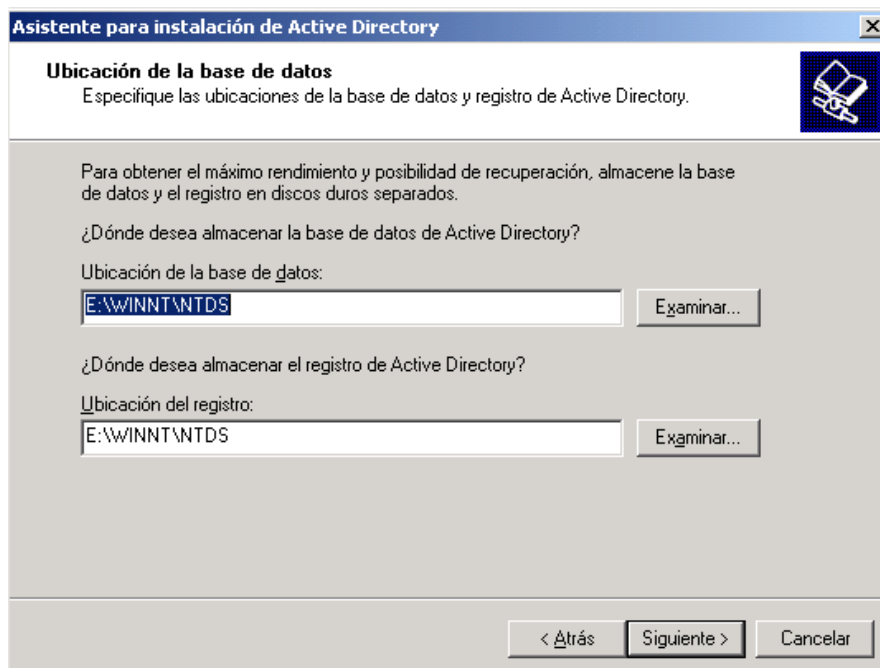
A continuación se muestra la pantalla Nombre de dominio NetBIOS. Después de introducir un nombre DNS para el dominio, el sistema solicita un equivalente NetBIOS para el nombre del dominio para que los utilicen los clientes que no soporten Active Directory. Los sistemas Windows 2000 todavía utilizan el espacio de nombres NetBIOS para sus nombres de equipo, pero Active Directory utiliza la nomenclatura DNS para los dominios. Windows NT 4 y los sistemas Microsoft Windows 9x utilizan nombres NetBIOS para todos los recursos de la red, incluyendo los dominios.

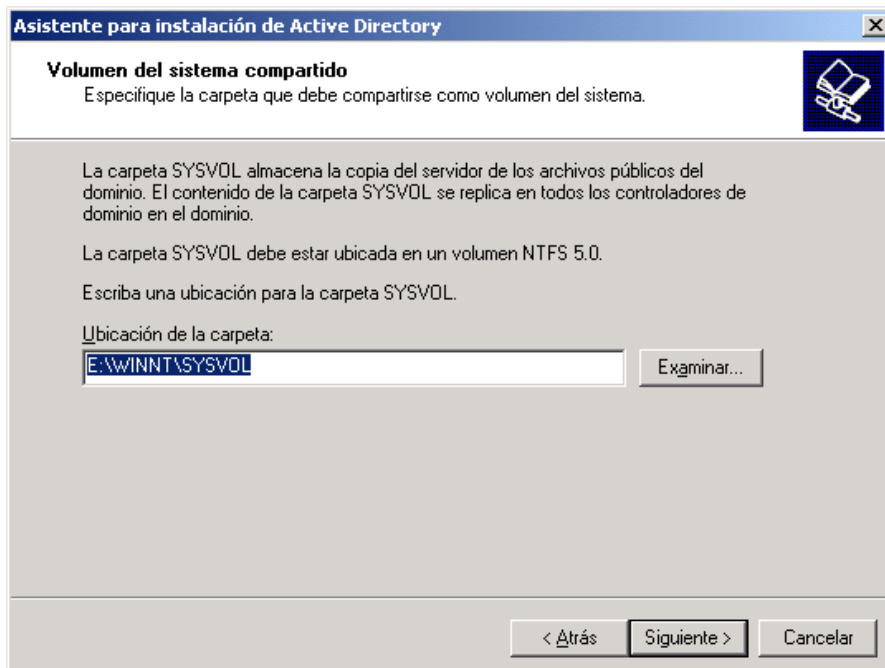
Si se dispone de clientes de nivel inferior en la red (esto es, Windows NT 4, Windows 9x, Microsoft Windows para Trabajo en grupo o Cliente de red Microsoft para sistemas MS-DOS), estos solo serán capaces de ver el nuevo dominio por medio del nombre NetBIOS. La pantalla Nombre de dominio NetBIOS contendrá una sugerencia para el nombre, basándose en el nombre DNS especificado, que se puede utilizar o bien se puede reemplazar con un nombre que se elija que tenga 15 caracteres o menos.



Deje el nombre propuesto automáticamente como nombre NetBIOS y haga clic en Siguiete.

Después de especificar los nombres de dominio, el asistente solicita las ubicaciones de la base de datos, los archivos de registro y el volumen del sistema de Active Directory.





La base de datos de Active Directory contendrá los objetos Active Directory y sus propiedades, mientras que los archivos de registro registran las actividades del servicio de directorio. Los directorios para estos archivos se especifican en la pantalla ubicación de la base de datos. La ubicación predeterminada tanto para la base de datos como para los registros es la carpeta %SystemRoot%\Ntds del volumen del sistema, pero se pueden modificar según nuestras necesidades siendo aconsejable que no residieran en el mismo disco que el sistema operativo.

La pantalla Volumen del sistema compartido permite especificar la ubicación de lo que se convertirá en el recurso compartido Sysvol del controlador de dominio. El volumen del sistema es un recurso compartido que contiene información del dominio que se replica al resto de controladores de dominio de la red. De forma predeterminada, el sistema crea este recurso compartido en la carpeta %SystemRoot%\Sysvol en la unidad de disco del sistema. La base de datos, los registros y el volumen del sistema de Active Directory tiene que situarse en volúmenes que utilicen el sistema de archivos NTFS 5. Si el asistente detecta que alguno de los volúmenes escogidos no utiliza NTFS 5, habrá que convertirlos o seleccionar otro volumen antes de poder completar el proceso de instalación de Active Directory. También resulta aconsejable situarlo en otro disco distinto al del sistema operativo.

A continuación se completa la instalación de DNS. En este punto, el Asistente para instalación de Active Directory tiene toda la información de configuración necesaria para instalar Active Directory y promover el servidor a controlador de dominio. El sistema comprueba que los nombres de dominio suministrados no los utiliza ya un servidor DNS en otros equipos de la red. Si, por ejemplo, el nombre NetBIOS seleccionado ya lo está utilizando un dominio Windows NT 4 en la red, el asistente pide que se seleccione otro nombre.

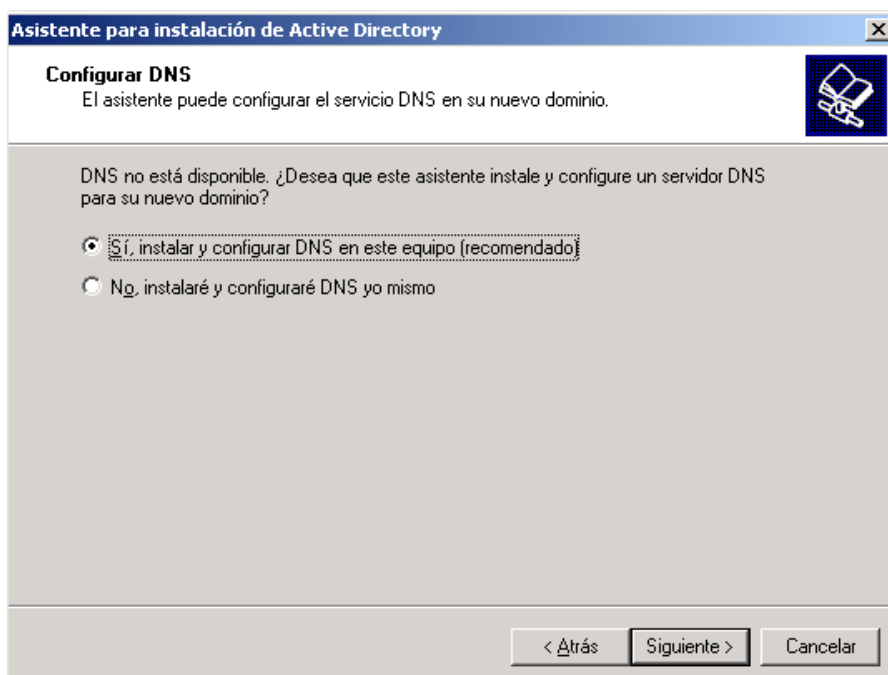


El asistente también determina si el servidor DNS que alojara el dominio soporta el protocolo de Actualización dinámica.



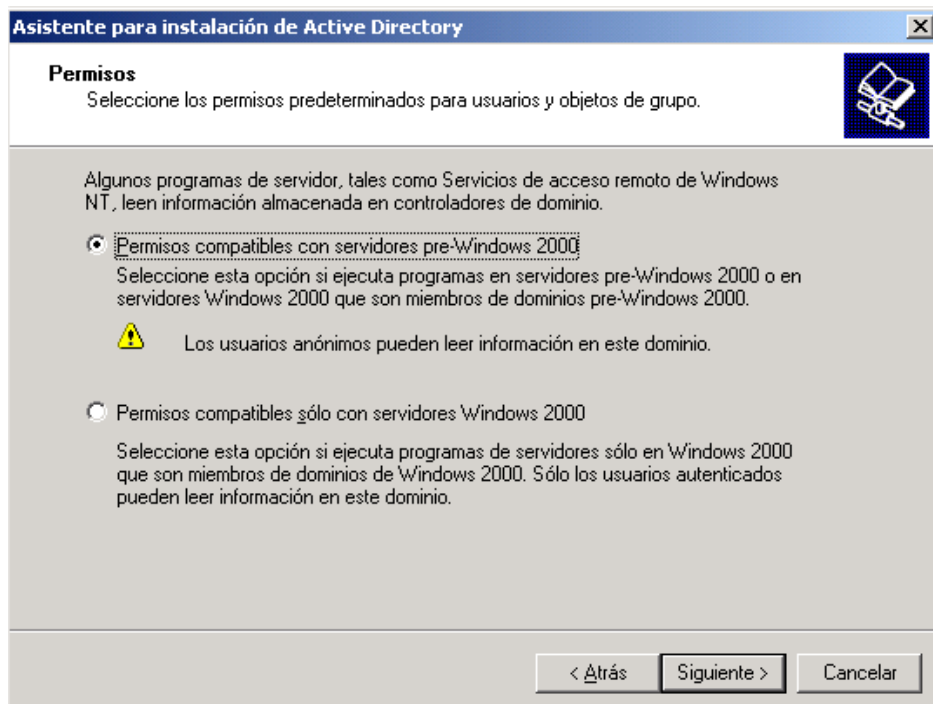
Si el sistema no puede contactar con el servidor DNS especificado en la configuración TCP/IP cliente del equipo, o si el servidor DNS especificado no es capaz de dar soporte a un dominio Windows 2000, el asistente se ofrece a instalar Microsoft DNS Server y configurarlo para que funcione como servidor autorizado para el dominio. La pantalla Configurar DNS permite especificar si se desea instalar el servidor DNS o configurar uno personalmente. Si se opta por utilizar otra máquina para el servidor DNS, es preciso instalarlo y configurarlo antes de poder completar la instalación de Active Directory.

Elija la opción Sí, instalar y configurar DNS en este equipo (recomendado).

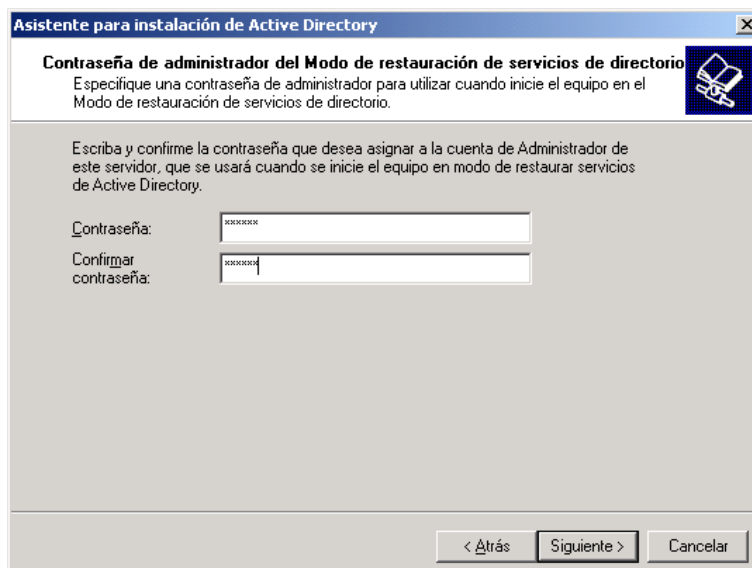


Haga clic en Siguiente.

La siguiente ventana presenta la configuración de Permisos que le permite configurar la compatibilidad con versiones de servidores previas a Windows 2000.

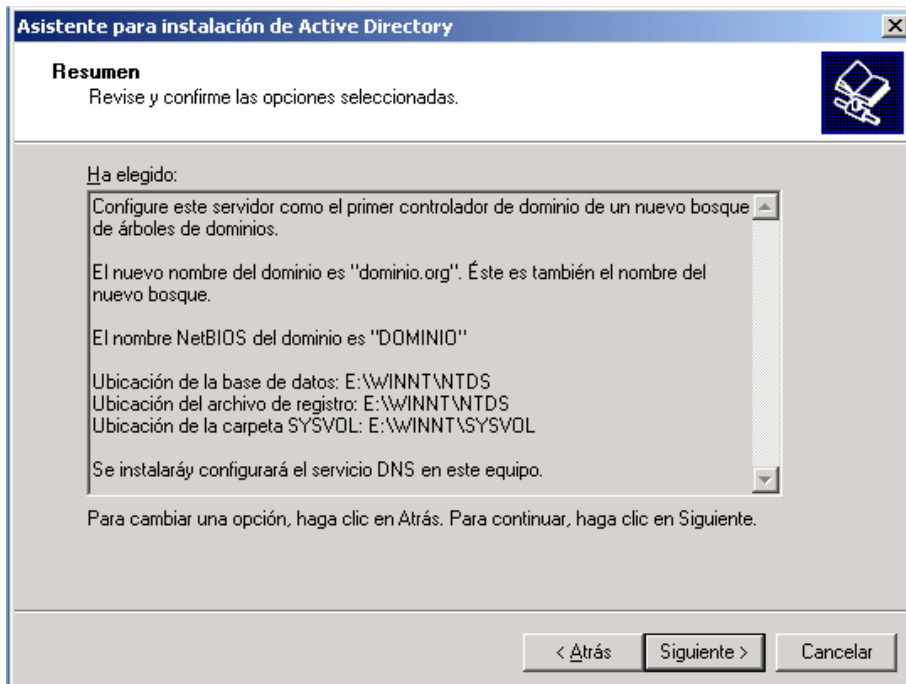


Debido a que en nuestra red sólo habrá servidores Windows 2000, elija la segunda opción, Permisos compatibles sólo con servidores Windows 2000. En la siguiente ventana, se solicita que introduzca la información de contraseña para la cuenta administrador de Active Directory. Ésta puede ser distinta a la utilizada para la cuenta de administrador del equipo local, y es recomendable utilizar una contraseña distinta.



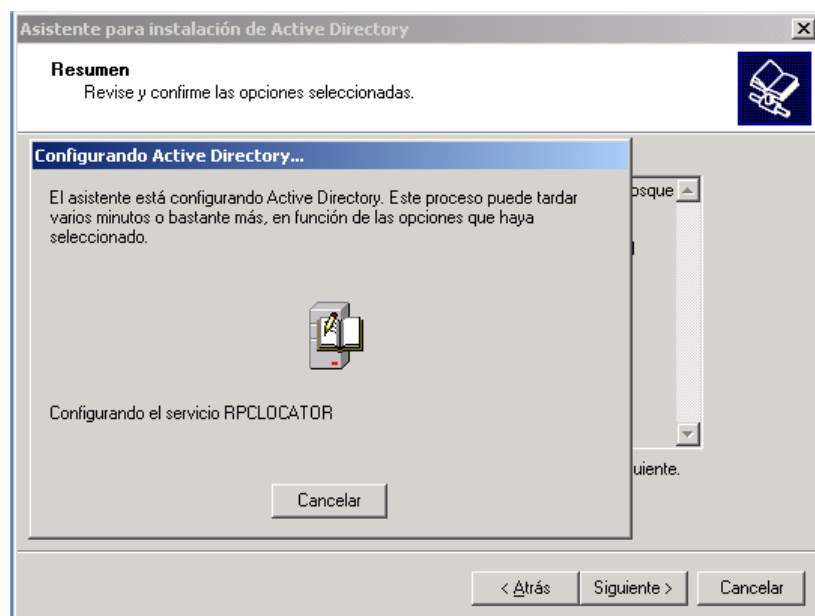
En este caso utilizaremos la contraseña alumno.

Por último se presenta la pantalla de resumen de la configuración. Si se encuentra algún error es posible retornar para corregirlo en este momento.



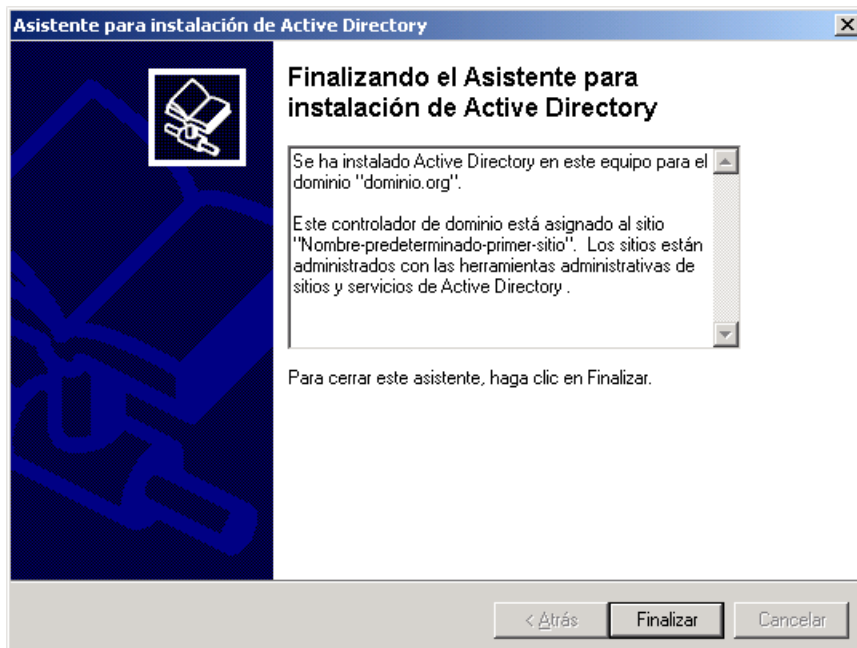
Si toda la información es correcta, haga clic en Siguiendo.

A continuación comienza el proceso de finalización de la instalación de Active Directory. Después de que el asistente contacte con el servidor DNS que proporcionara el servicio localizador para el nuevo dominio, se completa la instalación y configuración de Active Directory sin más introducción de datos por parte del usuario. El asistente registra todas las actividades que se producen durante el proceso de instalación en dos archivos llamados Dcpromo.log y Dcpromoui.log, localizados en la carpeta %SystemRoot%\debug.

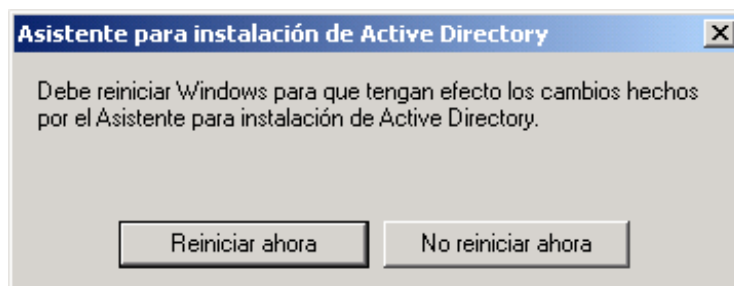




La instalación puede durar varios minutos, después de lo cual hay que reiniciar el sistema para que tengan efecto los cambios.



Reinicie el equipo cuando se le solicite.



Paso 3 Servidor de catálogo global

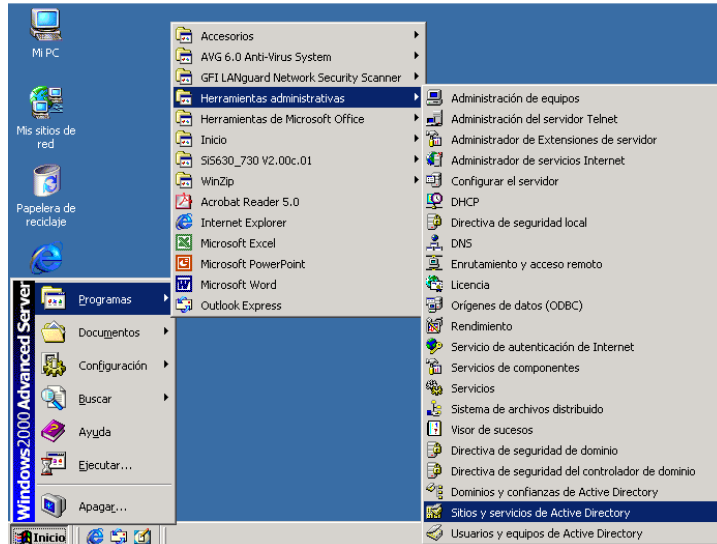
El primer controlador de dominio Windows 2000 de un bosque es automáticamente un servidor de Catálogo global. El Catálogo global (CG) contiene una réplica completa de todos los objetos de directorio del dominio en que se aloja además de una replica parcial de todos los objetos de directorio de cada dominio del bosque. El objetivo de un CG es proporcionar autenticación a los inicios de sesión. Además, como un CG contiene información sobre todos los objetos de todos los dominios del bosque, la búsqueda de información en el directorio no requiere consultas innecesarias a los dominios. Una única consulta al CG produce la información sobre donde se puede encontrar el objeto.

De forma predeterminada, habrá un CG, pero cualquier controlador de dominio se puede configurar como servidor de Catalogo global. Si se necesitan servicios de inicio de sesión y búsqueda adicionales, se pueden tener múltiples servidores de Catalogo global en el dominio.

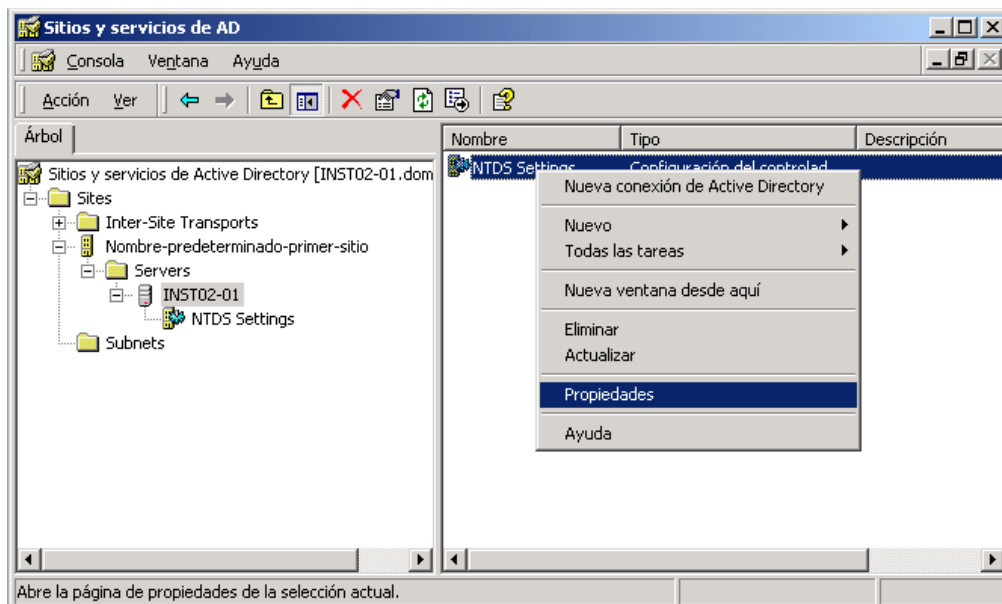


Para convertir un controlador de dominio en un servidor de Catalogo global, hay que seguir los siguientes pasos.

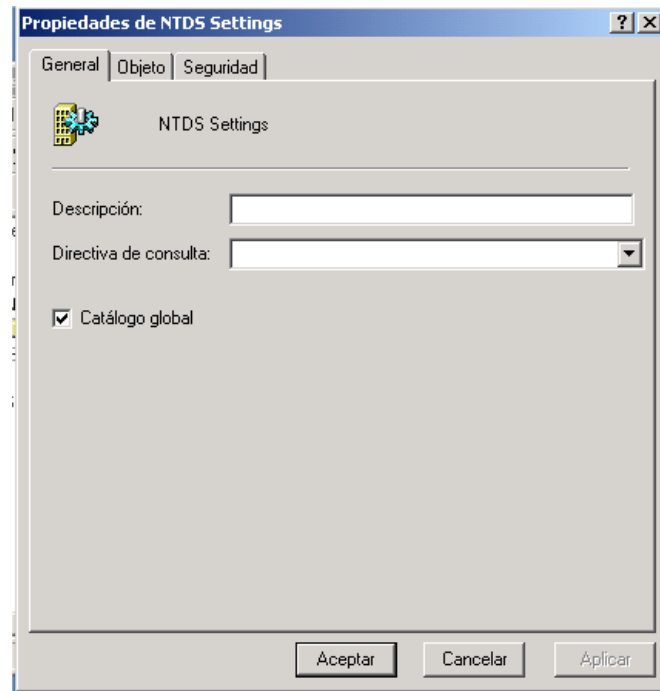
- 1- Escoger Sitios y servicios de Active Directory en el menú Herramientas administrativas (Inicio => Programas => Herramientas Administrativas => Sitios y Servicios de Active Directory).



- 2- Abrir Sites y seleccionar el sitio correspondiente.
- 3- Abrir Servers y seleccionar después el controlador de dominio que se desea convertir en servidor de Catalogo global.
- 4- Seleccionar NTDS Settings en el panel derecho y escoger propiedades en el menú Acción.



En la pestaña General, seleccionar la casilla de verificación Catalogo global.

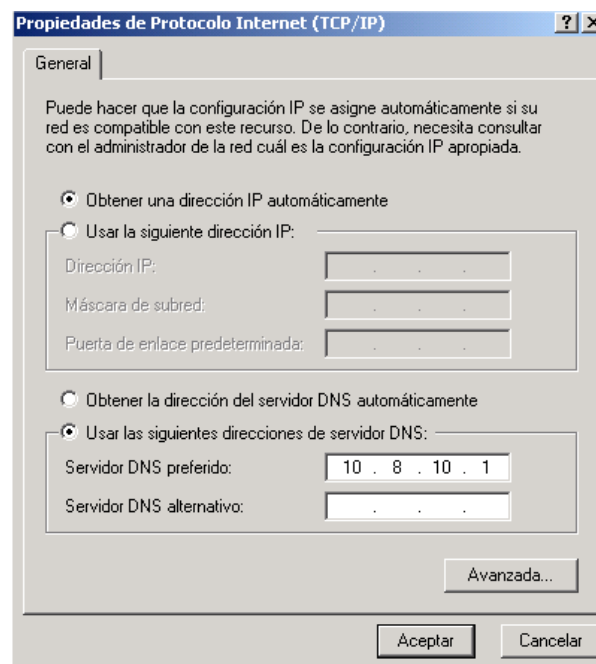


Paso 4 Agregar un cliente al dominio

Desde una PC cliente con Windows 2000 Professional, configure para agregarlo al dominio.

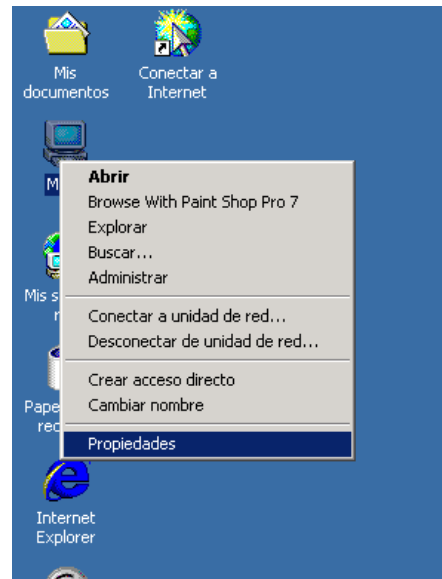
Primero, inicie sesión como Administrador de la máquina local utilizando la contraseña alumno.

A continuación configure en las propiedades de Mis Sitios de red, la dirección IP del servidor DNS del controlador de dominio (por ejemplo, 10.2.110.1).

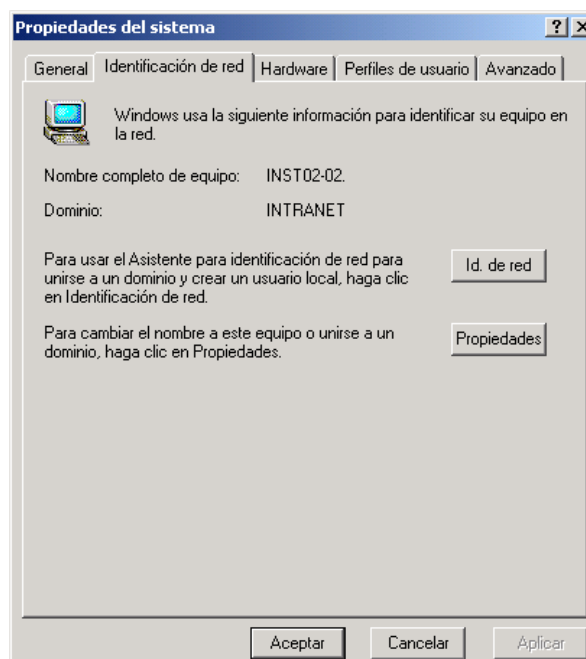




Acepte las ventanas de configuración de red y a continuación seleccione el icono Mi PC, haga clic con el botón derecho del mouse y seleccione Propiedades.

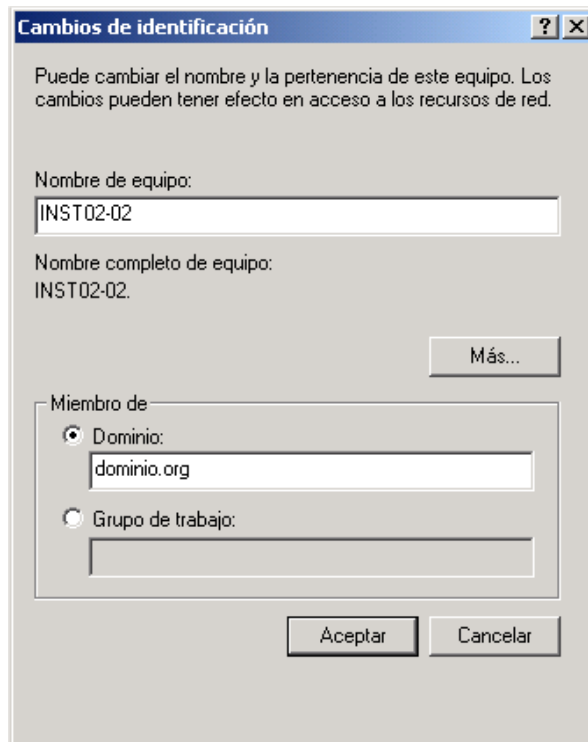


Cuando se abra la ventana de Propiedades del Sistema, seleccione la pestaña Identificación de Red.

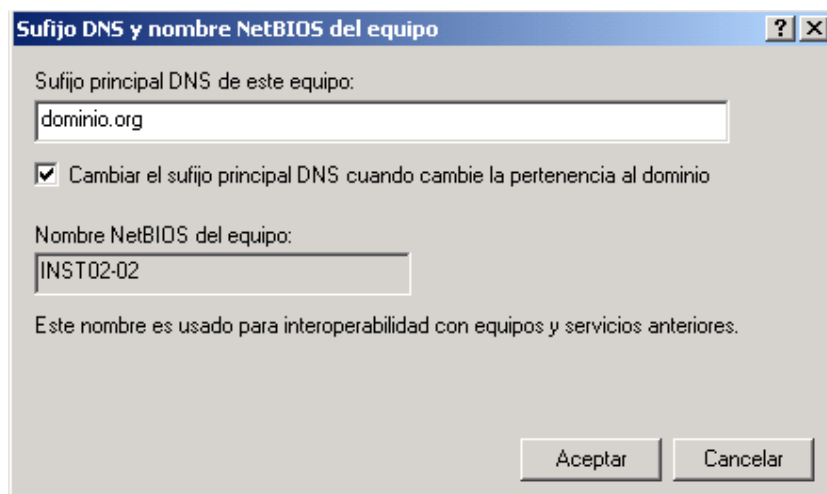


Seleccione el botón Propiedades. Se abre la ventana Cambios de identificación.

En el campo dominio, ingrese la información del dominio que configuró anteriormente en el servidor (por ejemplo, grupo1.org, grupo2.org, etcétera).

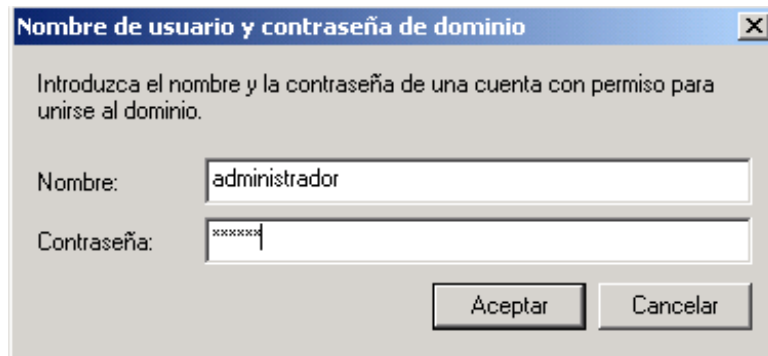


Haga clic en el botón etiquetado Más ... y en el campo Sufijo principal DNS de este equipo configure el nombre de dominio (por ejemplo grupo1.org).



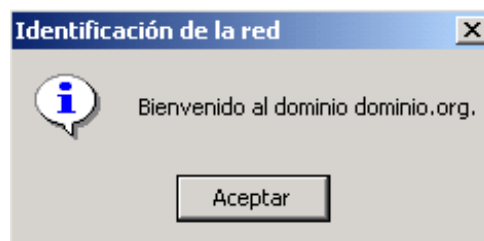
Acepte la ventana de configuración de Sufijo DNS y nombre NetBIOS del equipo y acepte la ventana de Cambios de configuración.

A continuación se presentará una ventana solicitándole la información de una cuenta de usuario y contraseña con permiso para unir la PC al dominio.

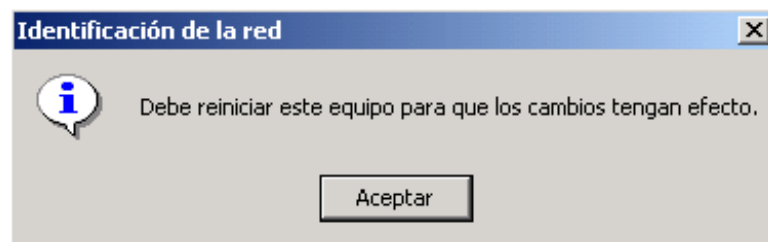


Utilice el nombre de usuario administrador con la contraseña alumno.

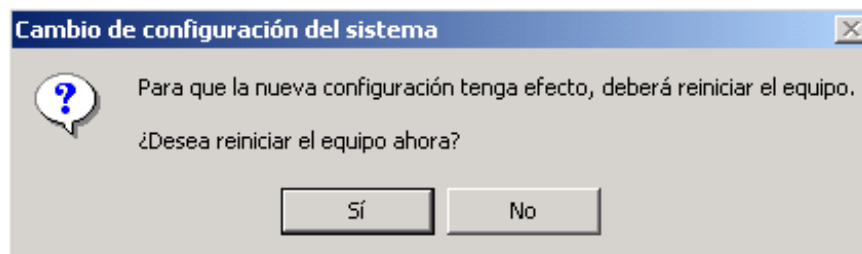
Si esta información es correcta, se mostrará un mensaje dando la bienvenida al nuevo dominio.



Acepte la ventana y a continuación se le solicitará que reinicie el equipo.



Haga clic en Aceptar para que se reinicialice. Acepte la ventana de configuración de Cambios de identificación y haga clic en el botón Si cuando se le solicite reiniciar ahora.



Paso 5 Prueba de funcionamiento

En la PC cliente, luego de reiniciar el equipo, inicie una sesión en el dominio.



Como aún no se han creado usuarios pertenecientes al dominio, utilice la información de la cuenta del administrador para loguearse.

¿Tuvo éxito?

En el equipo Controlador de dominio, abra la consola de administración de DNS (Inicio => Programas => Herramientas Administrativas => DNS).

Despliegue el árbol de DNS hasta la zona de búsqueda y seleccione el nombre de dominio que configuró anteriormente. En la pantalla de la derecha deben listarse los nombres de hosts mapeados a sus respectivas direcciones IP.

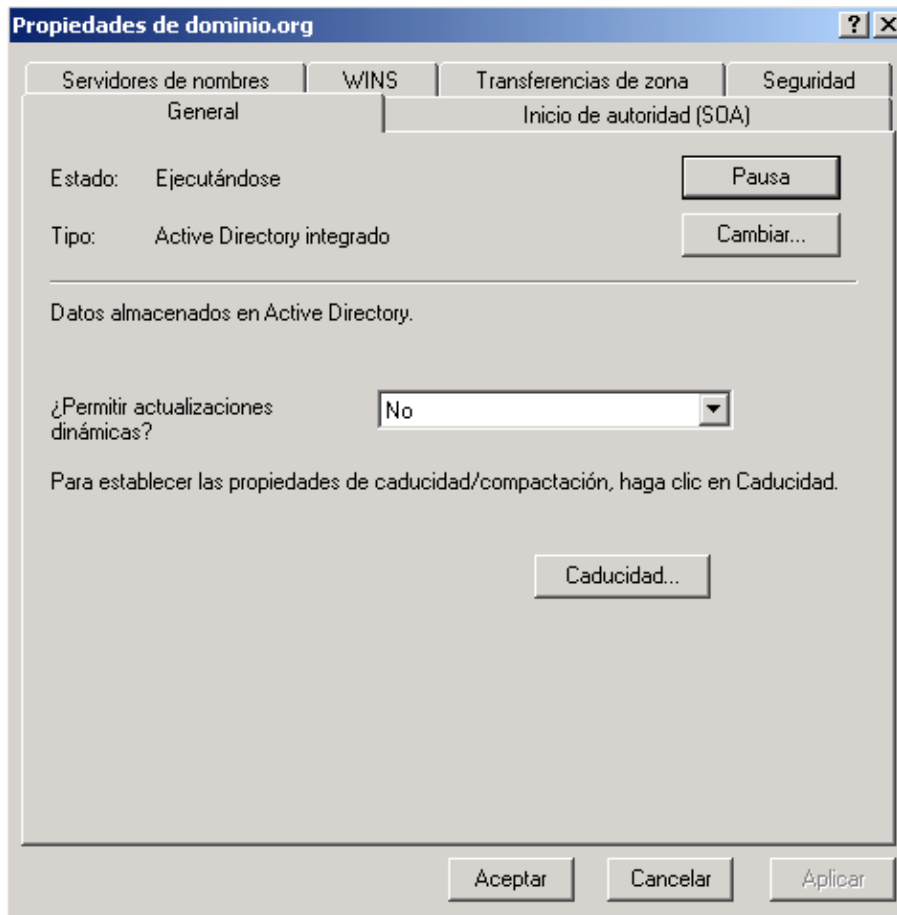
¿Se encuentra la PC cliente?

Abra la consola de administración de Usuarios y Equipos de Active Directory (Inicio => Programas => Herramientas Administrativas => Usuarios y Equipos de Active Directory). En el árbol del dominio, seleccione Computers.

¿Se lista la PC cliente?

Paso 6 Administración de equipos

En el equipo que es controlador de dominio, abra la consola de administración de DNS. Seleccione el nombre de dominio que está administrando (por ejemplo, grupo1.org) y seleccione Acción => Propiedades.



En la pestaña General, en la pregunta ¿Permitir actualizaciones dinámicas?, seleccione la opción No.

Acepte la ventana.

En la ventana de la derecha se listan los nombres de equipos que están autorizados a iniciar sesión. Borre el nombre del equipo cliente (botón derecho sobre el nombre del equipo => Eliminar).

Abra la consola de administración de Usuarios y equipos de Active Directory. Seleccione en el árbol de la izquierda, debajo del nombre del dominio, Computers.

En la ventana de la derecha se listan los equipos del dominio. Elimine el nombre de equipo del cliente.

Paso 7 Prueba de funcionamiento

En el equipo cliente, cierre la sesión si esta está abierta y vuelva a iniciar utilizando la misma información que la última vez que se logueó.

¿Pudo iniciar sesión?



¿Por qué?

Paso 8 Agregar el equipo cliente

En la PC cliente, inicie una sesión utilizando la cuenta de administrador local, abra las propiedades del sistema (botón derecho sobre MI PC => Propiedades). En la pestaña Identificación de red, seleccione Propiedades.

Agregue la PC al dominio correspondiente (por ejemplo, grupo1.org).

¿Tuvo éxito?

Paso 9 Examinar la información en el servidor

En el servidor controlador de dominio, abra Usuarios y equipos de Active Directory.

En el árbol del dominio, seleccione Computers. En la ventana de la derecha se listan los equipos miembros del dominio.

¿Está presente el nombre del equipo cliente?

Abra la consola de administración de DNS. En el árbol de DNS seleccione el dominio correspondiente (por ejemplo, grupo1.org). En la ventana de la derecha se listan los nombres de dominio con su correspondiente dirección IP.

¿Se encuentra la PC cliente?

Pruebe realizar un ping desde el servidor hacia la PC cliente.

```
ping nombre_PC.grupoX.org
```

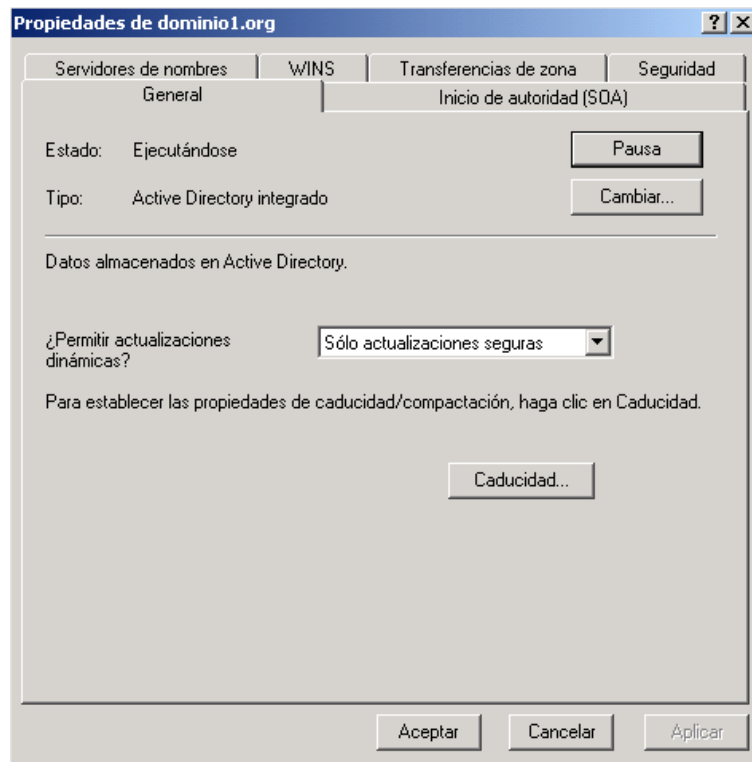
Donde nombre_PC es el nombre del equipo cliente y grupoX debe ser reemplazado por el dominio que configuró.

¿Tuvo éxito?

Paso 10 Configurar el servidor DNS



En el equipo controlador de dominio, abra la consola de administración de DNS. Sobre el dominio que está administrando (por ejemplo, grupo1.org) haga clic derecho y elija Propiedades.



En la pestaña General, en la consulta ¿Permitir actualizaciones dinámicas?, elija la opción Sólo actualizaciones seguras.

Acepte la ventana.

Paso 11 Actualizar el DNS

En el equipo cliente, abra una ventana de comandos (Inicio => Ejecutar => cmd). Típee el siguiente comando:

```
ipconfig /registerdns
```

Este comando debería actualizar la información del DNS.

Paso 12 Verificación del DNS

En el controlador de dominios, abra la consola de administración de DNS. Seleccione el dominio con el cual está trabajando. En el panel de la derecha, se listan los nombres de equipos y sus correspondientes direcciones IP.

¿Está el nombre del equipo cliente?

Abra una ventana de comandos y ejecute:



ping nombre_PC.grupoX.org

¿Tuvo éxito el ping?