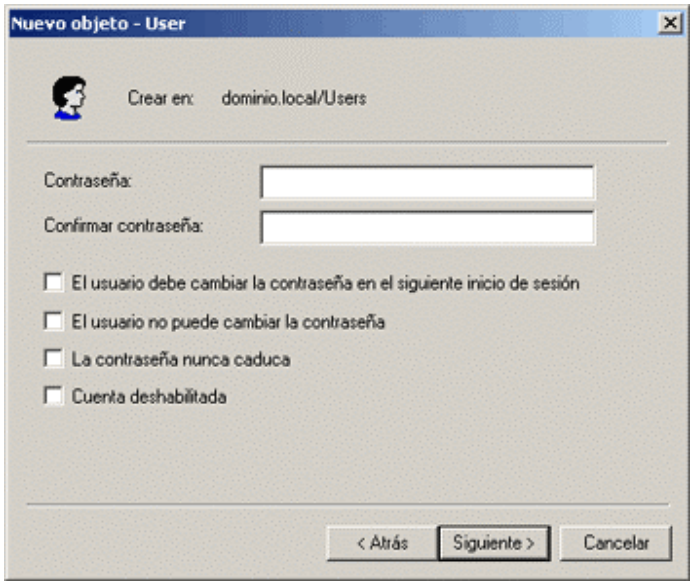
Tema 7°: ADMINISTRACIÓN Y GESTIÓN DE UNA LAN

1. *Agregación de Usuarios locales; perfil local*
2. *Implementación de dominios*
3. *Creación de una consola personalizada*
4. *Instalación del directorio activo*
5. *Usuarios globales; copiar cuentas de usuario*
6. *Grupos. Ámbito de un grupo*
7. *Equipos. Cuentas de equipo*
8. *Directorios. Permisos a carpetas compartidas*
9. *Establecimiento de permisos de toma de posesión*
10. *Dominios y confianzas del Directorio Activo*
11. *Tipos de objetos del Directorio Activo*
12. *Creación de Unidades Organizativas*
13. *Creación de objetos equipo*
14. *Publicación de carpetas compartidas*
15. *Publicación de impresoras*
16. *Traslado, cambio de nombre y eliminación de objetos*
17. *Derechos de usuario*

7.1.- Agregación de usuarios locales; Perfil Local

Una instalación típica de Active Directory consiste normalmente en mas objetos usuario que de cualquier otro tipo, y la creación y gestión de los objetos usuario representa buena parte de la carga de administración de Active Directory. La tarea de crear manualmente un objeto usuario es idéntica a la de la creación de una unidad organizativa o cualquier otro objeto. después de seleccionar el contenedor en el que residirá el objeto usuario (normalmente, una OU), hay que seleccionar el contenedor y escoger Nuevo en el menú acción y seleccionar Usuario, o pulsar el botón Crear un nuevo usuario de la barra de herramientas de Usuarios y equipos de Active Directory, lo que produce el cuadro de dialogo.



En el cuadro de dialogo Nuevo objeto, hay que especificar el nombre y apellidos del usuario y el nombre de inicio de sesión que proporcionara el usuario cuando se conecte a la red. El nombre de inicio de sesión de nivel inferior para el usuario (esto es, el nombre con el que iniciara sesión

el usuario en las estaciones de trabajo Windows NT o Windows 9.x) aparece entonces automáticamente. El siguiente cuadro de dialogo proporciona un campo para la contraseña del objeto usuario y permite establecer opciones básicas para la contraseña y la cuenta para el usuario, como sigue:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
- El usuario no puede cambiar la contraseña.
- La contraseña nunca caduca.
- Cuenta deshabilitada.

Después de que una pantalla de resumen confirme la información introducida, Usuarios y equipos de Active Directory crea el objeto usuario en el contenedor seleccionado.

Configuración de los objetos usuario

Una vez que se ha creado un objeto usuario, se puede proceder con el proceso de configuración, en el cual se añade información sobre el usuario a la base de datos de Active Directory y se define el acceso a la red del usuario. El menú Acción que genera Usuarios y equipos de Active Directory cuando se pulsa sobre un objeto usuario contiene algunos de los comandos mas comúnmente utilizados por los administradores, además del acceso a la ventana Propiedades del usuario. Estos comandos son los siguientes:

- **Agregar miembros a un grupo** Genera un cuadro de dialogo desde el que se pueden seleccionar los grupos a los que pertenecerá el usuario.
- **Asignaciones de nombres** (Solo visible cuando están activas las Características avanzadas.) Permite a los administradores asignar certificados X.509 y nombres Kerberos al objeto usuario.
- **Deshabilitar cuenta** Impide que el usuario inicie sesión en la red utilizando la cuenta hasta que sea activada manualmente por un administrador.
- **Restablecer contraseña** Genera un cuadro de dialogo con el que se puede modificar la contraseña de inicio de sesión de la cuenta del usuario.
- **Mover Permite** a los administradores trasladar el objeto usuario a otro objeto contenedor (esto es, un dominio o una unidad organizativa) de Active Directory.
- **Abrir la página principal** Abre el navegador predeterminado del sistema y muestra el URL que aparece en el campo Página Web de la pestaña General de la ventana Propiedades del objeto usuario.
- **Enviar mensaje de correo** Abre el cliente de correo electrónico predeterminado del sistema y escribe la dirección de un mensaje utilizando la dirección de correo

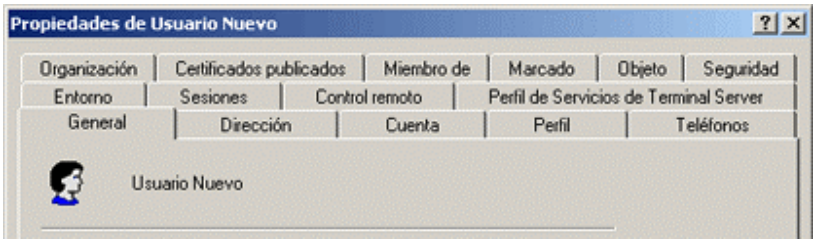
electrónico que aparece en el campo Correo electrónico de la pestaña General de la ventana Propiedades del objeto usuario.

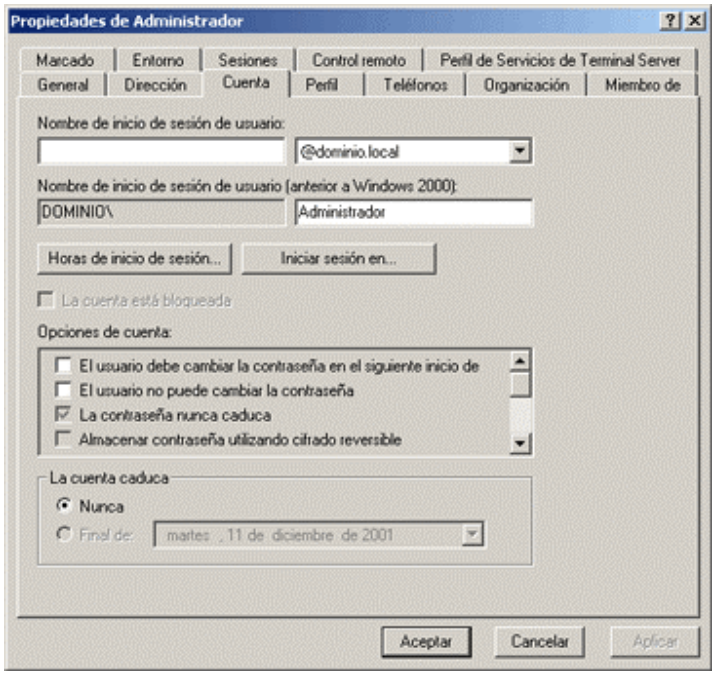
Aunque Usuarios y equipos de Active Directory proporciona estas funciones en el menú Acción para que resulte mas cómodo, también se puede acceder a muchas de ellas a través de la ventana Propiedades del objeto usuario, que proporciona una interfaz completa para los atributos del objeto usuario.

Los atributos que aparecen en las pestañas de la ventana Propiedades son aquellos incluidos en el esquema predeterminado que utiliza Active Directory. Se puede modificar el esquema para crear atributos adicionales o cambiar los existentes utilizando el complemento Administrador del Esquema de Active Directory.

La pestaña General

La pestaña General contiene información básica sobre el usuario, incluyendo el nombre y apellidos que se especificaron al crear el objeto. Esta pestaña también posee campos para una frase descriptiva sobre el usuario, la ubicación de la oficina, el número de teléfono, la dirección de correo electrónico y el URL de la página Web del usuario. Aparte de los campos nombre, la información de esta pestaña es opcional y únicamente se utiliza como referencia. Los usuarios pueden buscar en Active Directory utilizando los valores de los atributos de esta (y otras) pestañas y la dirección de correo electrónico y el URL de la página Web del usuario se insertan automáticamente en las aplicaciones cliente apropiadas, pero estos campos no afectan al acceso a la red del usuario de ninguna forma palpable.





La pestaña dirección

En la pestaña dirección se encuentran los campos donde se puede insertar la información de la dirección de correo del

usuario. Como en la pestaña General, estos son campos de referencia que no juegan un papel importante en la configuración del objeto.

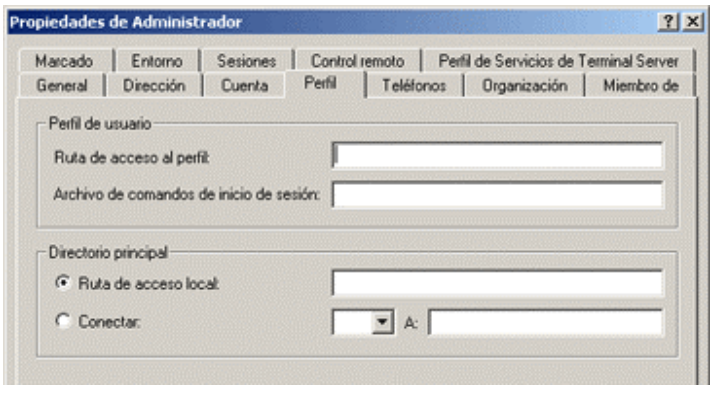
La pestaña Cuenta

La pestaña Cuenta contiene el nombre de inicio de sesión de usuario que se especificó durante la creación del objeto además de su nombre de usuario de nivel inferior.

Los botones Horas de inicio de sesión a Iniciar sesión en proporcionan acceso a cuadros de dialogo que permiten restringir las horas y días de la semana a los que tiene permiso el usuario para iniciar sesión en la red y las estaciones de trabajo desde las que el usuario puede iniciar sesión en la red.

La casilla de verificación La cuenta esta bloqueada esta seleccionada si la cuenta del usuario ha sido desactivada, bien deliberadamente por un administrador o a causa de repetidos fallos al iniciar sesión. Desactivar esta casilla libera la cuenta y permite al usuario iniciar sesión de nuevo. El área Opciones de cuenta contiene numerosas opciones para la contraseña y la cuenta (algunas de las cuales están duplicadas en el cuadro de dialogo Nuevo objeto). Cuando se crean nuevas cuentas de usuario, las siguientes opciones deben ser seleccionadas o desactivadas:

- **El usuario debe cambiar la contraseña en el siguiente inicio de sesión** Presenta al usuario un cuadro de dialogo en el siguiente inicio de sesión requiriéndole una nueva contraseña.
- **El usuario no puede cambiar la contraseña** Impide que el usuario cambie su propia contraseña.
- **La contraseña nunca caduca** Impide que la cuenta de usuario sea objeto de las directivas s de caducidad definidas en el cuadro La cuenta caduca.
- **Cuenta deshabilitada** Impide que el usuario inicie sesión utilizando esta cuenta hasta que la casilla sea desactivada por un administrador.



La pestaña Perfil

En la pestaña Perfil se puede especificar la ubicación del perfil de usuario asociado con el objeto. De forma predeterminada, cada usuario que inicia sesión en un sistema Windows 2000 tiene un directorio de perfil creado en la carpeta Documents and Settings de la unidad de disco del sistema. Cuando se especifica una ruta de acceso al perfil en esta pestaña, el sistema almacena

una copia del perfil en el directorio especificado. Si este directorio esta localizado en una unidad de red compartida, el usuario puede acceder al perfil desde cualquier sistema de la red. El campo Archivo de comandos de inicio de sesión especifica el nombre del archivo de comandos que la estación de trabajo debería ejecutar cuando el usuario inicie sesión en la red.

Desde el cuadro Directorio principal, se puede crear un directorio personal en una unidad de red sobre el que el usuario tendrá control completo. Almacenar los archivos de datos en una unidad de red facilita su protección ante manipulaciones y los borrados accidentales. Se puede configurar la estación de trabajo para que asigne una unidad a la unidad de disco compartida automáticamente durante el proceso de inicio de sesión especificando una letra de unidad y el nombre UNC de un recurso compartido de la red en los campos Conectar. En el campo para indicar la carpeta de documentos compartidos, se puede especificar una ubicación donde los usuarios que requieren acceso a los mismos documentos pueden almacenar archivos.

La pestaña Teléfonos

La pestaña Teléfonos contiene campos para los distintos números de teléfono asociados con un usuario, incluyendo los números del localizador, del móvil, del fax y del teléfono de IP Un campo Notas de múltiples líneas proporciona un área de propósito general para notas.

La pestaña organización

La pestaña Organización proporciona campos en los que se puede especificar el titulo, el departamento y la organización del usuario. En el cuadro Administrador, se puede identificar el superior del usuario seleccionando otro objeto usuario de Active Directory. Un campo **Supervisa a**, de múltiples líneas permite almacenar las notas de un supervisor en el usuario.

La pestaña Miembro de

La pestaña Miembro de es donde se especifican los grupos de los que el usuario debería ser miembro. Si se pulsa el botón Agregar, se muestra una lista de objetos desde la que se pueden seleccionar los grupos apropiados. El botón Establecer grupo solo esta activo para usuarios de Macintosh. Los Servicios para Macintosh de Windows reconocen una afiliación de grupo única, normalmente el grupo con el que los usuarios de Macintosh comparten documentos en un servidor.

También se puede añadir un usuario a un grupo desde la pestaña Miembros de la ventana Propiedades de un objeto grupo.

La pestaña Marcado

En la pestaña Marcado se controla si al usuario se le permite el acceso a la red a través de una conexión telefónica del Servicio de acceso remoto (RAS, Remote Access Service). Con la opción Permitir acceso se puede seleccionar si el objeto usuario necesita devolución de

llamada o el Id del que llama para la comprobación de seguridad, y se pueden especificar una dirección IP estática y rutas estáticas para la conexión.

La pestaña Certificados publicados

La pestaña Certificados publicados, que solo es visible cuando se activa la opción de presentación Características avanzadas de Usuarios y equipos de Active Directory, permite administrar los certificados X.509 vinculados al objeto usuario. Desde esta página se pueden examinar los certificados publicados para la cuenta del usuario, agregar nuevos certificados, eliminar certificados y exportar certificados a archivos.

La pestaña Objeto

La pestaña Objeto muestra la ruta de acceso completa al objeto usuario, las fechas de su creación y ultima modificación y los números de secuencia de actualización (USN, Update Sequence Number) de su creación y ultima modificación.

La pestaña Seguridad

La pestaña Seguridad (visible solo cuando están activas las Características avanzadas) permite asignar permisos que controlan el acceso al objeto usuario. La pestaña es virtualmente idéntica a la misma pestaña de las ventanas propiedades de otros tipos de objetos.

Creación del Perfil Local:

Una cuenta local no puede acceder al dominio y, por lo tanto, solo tiene acceso a los recursos del equipo donde se crea y utiliza. Para crear una cuenta de usuario local hay que seguir estos pasos:

1. Pulsar con el botón derecho del ratón en Mi PC y escoger administrar en el menú contextual.
2. En el árbol de la consola, hay que pulsar Usuarios locales y grupos. Pulsar con el botón derecho del ratón en Usuarios y escoger Usuario nuevo en el menú contextual.
3. En el cuadro de dialogo Usuario nuevo hay que suministrar el nombre de usuario, el nombre completo y la descripción.
4. Proporcionar una contraseña y definir las directivas de contraseñas. Pulsar Crear. Las cuentas locales pueden pertenecer a grupos creados localmente (en el equipo único).

7.2.- Implementación de Dominios

Un dominio de Active Directory es un grupo e equipos que comparten una base de datos de directorio común.

Existen dominios padre y dominios secundarios. Si se forma parte de una red privada el nombre de dominio no debe entrar en conflicto con los nombres ya existentes en la red y si forma parte de Internet el nombre de dominio no debe entrar en conflicto con ningún otro dominio existente ya en Internet.

Cada dominio tiene sus propias directivas de seguridad y relaciones de confianza, los dominios se puede expandir a través de mas de una localización física, ósea que el dominio puede estar presente en varios sitios y que estos sitios pueden tener distintas subredes.

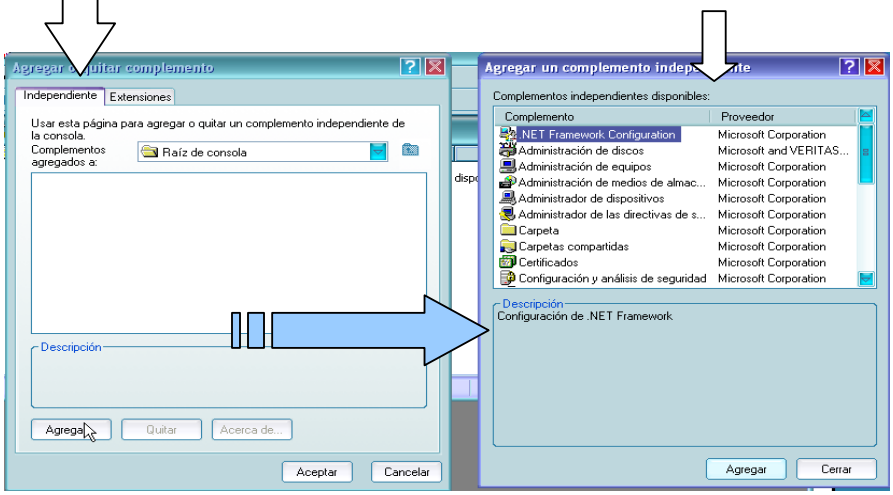
Dentro de la base de datos de directorio encontrara objetos que definen cuentas de usuario, grupos y equipos al igual que recursos compartidos, como impresoras o carpetas.

Cada dominio de Active Directory tiene nombre DNS, cuando uno o más dominios comparten los mismos datos de dirección, se denominan un bosque, los nombres de dominio dentro de este bosque pueden ser continuos o discontinuos en la jerarquía del DNS.

7.3.- Creación de una consola personalizada

En el botón de INICIO seleccionamos la opción EJECUTAR y escribimos "mmc", aparecerá el programa para crear la consola. Pulsamos en consola, agregar o quitar complemento, y le damos a agregar.

Aparecen una lista con todos los complementos independientes que se pueden agregar a nuestra consola. Se agregarán los que queramos.



Al crear una consola personalizada, puede asignar a la misma una o dos opciones de acceso generales: el modo de autor o el modo de usuario. Existen a su vez tres niveles en el modo de usuario, por lo que son cuatro las opciones para el acceso predeterminado a una consola:

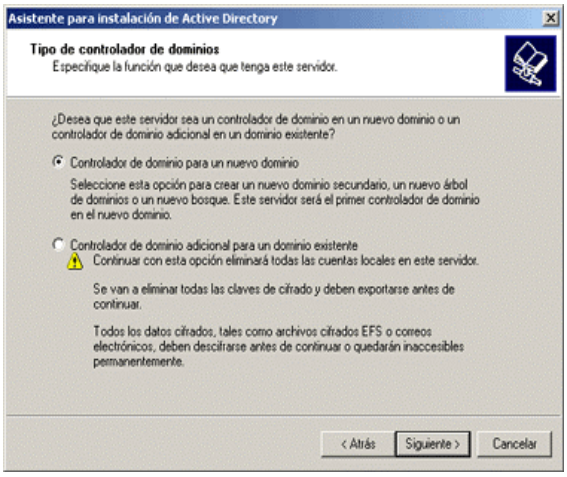
- Modo de autor
- Modo de usuario: acceso completo
- Modo usuario: acceso delegado, ventanas múltiples
- Modo usuario: acceso delegado, ventana única.

Puede configurar estas opciones en el cuadro de diálogo Opciones de MMC.

7.4.-Instalación del Directorio Activo

A diferencia de la versión 4 y anteriores de Microsoft Windows NT Server, Windows 2000 Server no designa un sistema como controlador de dominio durante la instalación del sistema operativo. Cada servidor de Windows 2000 se instala como un sistema independiente o un miembro de un dominio. Cuando la instalación esta completa se puede promocionar al servidor al estado de controlador de dominio utilizando el Asistente para instalación de Active Directory de Windows 2000. Esta herramienta proporciona una gran flexibilidad adicional a los administradores de Active Directory porque los servidores se pueden promover o degradar en cualquier momento, mientras que los servidores Windows NT 4 se designan irrevocablemente como controladores de dominio durante el proceso de instalación.

Algo que también ha desaparecido es la distinción entre controladores principales de dominio y controladores de dominio de reserva. Los controladores de dominio Windows 2000 son todos parejos en un sistema de réplica con múltiples maestros. Esto significa que los administradores pueden modificar los contenidos del árbol de Active Directory de cualquier servidor que funcione como controlador de dominio. Esto es un avance muy importante desde el sistema de réplica de un solo maestro de Windows NT 4, en el cual un administrador sólo puede cambiar el controlador principal de dominio (PDC, Primary Domain Controller) para que después los cambios se repliquen a todos los controladores de dominio de reserva (BDC, Backup Domain Controller).

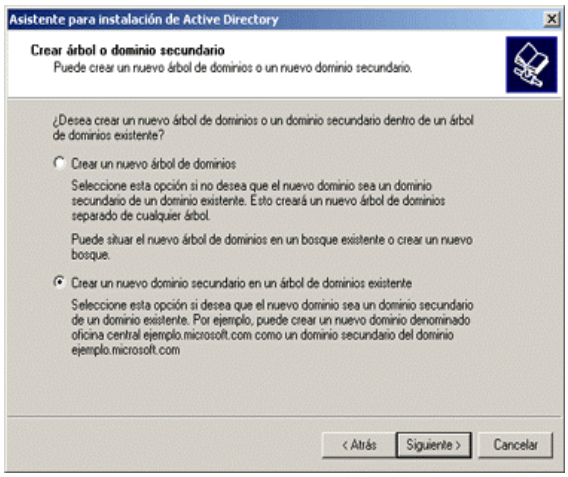


Otra ventaja de Windows 2000 es que se puede utilizar el Asistente para instalación de Active Directory para degradar un controlador de dominio de nuevo a un servidor independiente o miembro.

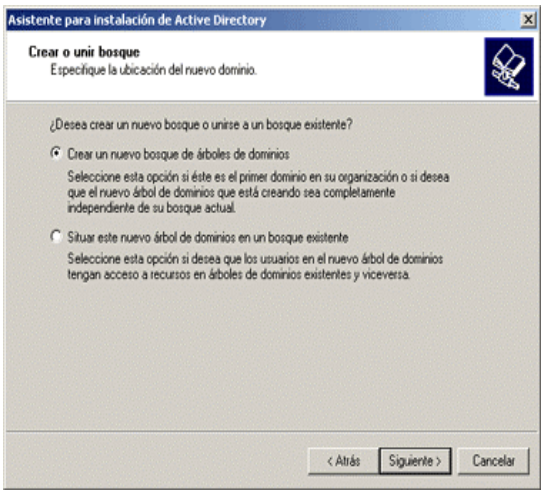
En Windows NT 4, una vez que se instala un servidor como controlador de dominio, es posible degradarlo de PDC a BDC, pero no se puede eliminar su estado de controlador de dominio completamente, excepto reinstalando el sistema operativo.

La función básica del Asistente para instalación de Active Directory es configurar un servidor para que funcione como controlador de dominio, pero dependiendo del estado actual de Active Directory en la red, esta tarea puede tomar distintas formas. Si se instala el primer Windows 2000 Server de la red, antes de la promoción del sistema a controlador de dominio crea un Active Directory completamente nuevo con esa computadora alojando el primer dominio del primer árbol del primer bosque.

La instalación comienza ejecutando desde el menú de inicio el comando DCPROMO.



Tipo de Controlador de Dominios: Después de una pantalla de bienvenida, 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 .

Crear árbol o dominio secundario. Deberemos 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 pare que aloje el primer dominio de un nuevo árbol.

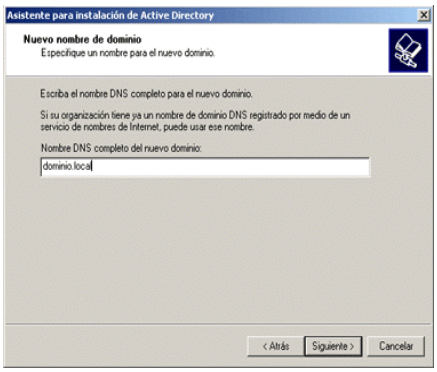
- **Crear un nuevo dominio secundario en un árbol de dominios existente:** Configura el nuevo controlador de dominio para que aloje un hijo de un dominio de un árbol que ya existe.

Crear o unir bosque, que permite especificar una de las siguientes opciones:

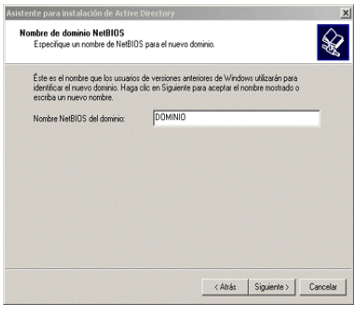
- **Crear un nuevo bosque de árboles de dominios:** Configura el controlador de dominio para que sea la raíz de un nuevo bosque de árboles.

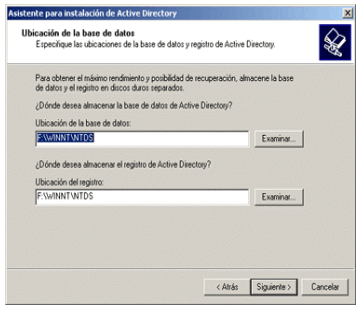
- **Situar este nuevo árbol de dominios en un bosque existente:** Configura el controlador de dominio para que aloje el primer dominio de un nuevo árbol en un bosque que ya contiene uno o más árboles.

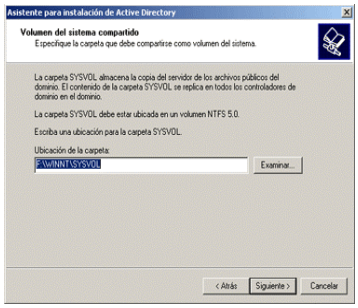
Nombre de nuevo Dominio: Para identificar el controlador de dominio en la red se debe especificar un nombre DNS valido para el dominio que se esta creando. Este nombre no tiene por que ser el mismo que el del dominio que utiliza la empresa para su presencia en Internet (aunque puede serlo). El nombre tampoco tiene que estar registrado en el Centro de información de redes de Internet (InterNIC, Internet Network información), 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.



Los Siguientes tres cuadros de dialogo no deben ser modificados, ya que los valores







que llevan implicitos por defecto son los recomendados.

Servidor DNS

El ultimo requisito para instalar Active Directory es que el servidor tenga acceso a un servidor DNS. Active Directory utiliza el DNS para almacenar información sobre los controladores de dominio de la red. Los sistemas cliente localizan un controlador de dominio para la autenticación mediante el envío de una petición al servidor DNS identificado en sus configuraciones TCP/IP cliente. El servidor DNS que utiliza Active Directory ni necesita estar ejecutándose en el equipo que se va a convertir en un controlador de dominio, ni tiene que ejecutar el servicio DNS de Microsoft.

Si no hay disponible en lo red un servidor DNS que soporte las nuevas características, el asistente se ofrecerá a instalar y configurar Microsoft DNS Server en el sistema automáticamente. Se puede rechazar la oferta a instalar un servidor DNS en otro sistema, pero el nuevo servidor debe ser capaz de acceder al servidor DNS para poder instalar Active Directory y promover el sistema a controlador de dominio.

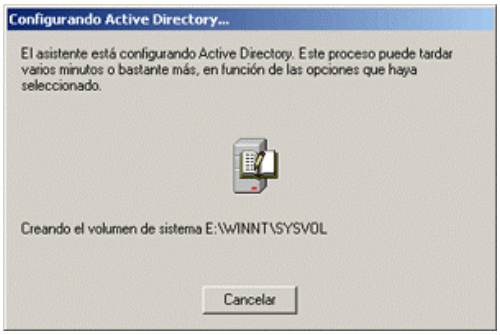
Debe tenerse en cuenta que:

1. Para identificar el controlador de dominio en la red se debe especificar un nombre DNS valido para el dominio que se esta creando. Este nombre no tiene por que 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 información), 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 use 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.

2. **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, qua se puede utilizar o bien se puede reemplazar con un nombre qua se elija qua tenga 15 caracteres o menos.

Si la red utiliza actualmente servidores DNS fuera del sitio para la resolución de nombres. Como los proporcionados por el proveedor de servicios Internet (ISP, Internet Service Provider), se debería instalar por lo menos un nuevo servidor DNS en la red local para dar soporte a Active Directory. Aunque los servidores DNS del ISO podrían soportar el registro de recursos Localización de servicios y el protocolo Actualización dinámica, es poco probable que los servidores Windows 2000 que se dispongan estén autorizados para actualizar dinámicamente los registros del servidor DNS del ISP E incluso si se permitiera, no resulta practico para los sistemas cliente atravesar un enlace WAN para solicitar información sobre recursos locales.



Una vez dados todos los pasos anteriores solo quedará asignar los permisos para dar acceso a servidores Windows NT 4 o solo a servidores con Windows 2000.

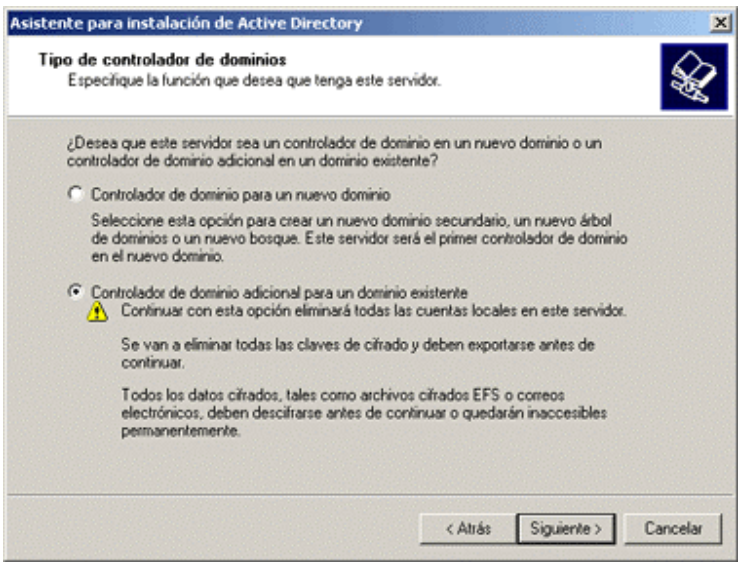
El siguiente paso será asignar la contraseña del administrador del nuevo dominio y confirmarla. A continuación pulsando el botón SIGUIENTE aparecerá un resumen con todos los parámetros que hemos ido asignando durante la instalación y solo quedará que el asistente configure el directorio activo.

Instalación de un Controlador de dominio de Réplica

Las replicas proporcionan tolerancia a fallos en un dominio Active Directory, y pueden reducir el trafico entre redes permitiendo a los clientes de la red autenticarse utilizando un controlador de dominio en el segmento local. Cuando un controlador de dominio no funciona correctamente o no esta disponible por algún motivo, sus replicas asumen automáticamente sus

funciones. Incluso un dominio pequeño necesita al menos dos controladores de dominio para mantener esta tolerancia a fallos.

Para crear una réplica de un dominio existente, hay que ejecutar el Asistente para instalación de Active Directory en un Windows 2000 Server recién instalado después de unirse al dominio que se trata de replicar. En el equipo que se une al dominio, se puede realizar la unión por primera vez y suministrar las credenciales administrativas que permiten al sistema crear un objeto equipo en el dominio, o bien se puede crear el objeto equipo manualmente por medio de Usuarios y equipos de Active Directory. Después de unirse al dominio, hay que iniciar sesión en el sistema utilizando la cuenta de administrador local y ejecutar el asistente desde la página Configurar el servidor o ejecutando Dcpromo.exe desde el cuadro de dialogo Ejecutar.



Cuando aparece la pantalla Tipo de controlador de dominios en el asistente, hay que seleccionar **Controlador de dominio adicional para un dominio existente** y especificar el nombre DNS del dominio que se va a replicar. Después hay que suministrar el nombre de usuario, la contraseña y el nombre de dominio de una cuenta con privilegios administrativos en el dominio.

El asistente instala Active Directory en el servidor, crea la base de datos, los registros y el volumen del sistema en las ubicaciones especificadas, registra el controlador de dominio en el servidor DNS y replica la información de un controlador de dominio para ese dominio existente.

Una vez que la replica del controlador de dominio esta en funcionamiento, no es distinguible del controlador de dominio existente, al menos en lo que concierne a la funcionalidad de los clientes. Las replicas funcionan como parejos, a diferencia de los servidores Windows NT, que están designados como controladores de dominio principales o de reserva. Los administradores pueden modificar el contenido de Active Directory (tanto los objetos como el esquema) de cualquier controlador de dominio, y los cambios se replicaran al resto de controladores de dominio de ese dominio.

Cuando se crea una replica, el Asistente para instalación de Active Directory configura automáticamente el proceso de replica entre los controladores de dominio. Se puede

personalizar el proceso de replica utilizando Sitios y servicios de Active Directory, que se incluye en Windows 2000 Server.

Establecimiento de un servidor de Catalogo global

El primer controlador de dominio Windows 2000 de un bosque es automáticamente un servidor de Catalogo global. El Catalogo global (CG) contiene una replica 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 estos pasos:

1. Escoger **Sitios y servicios de Active Directory** en el menú Herramientas administrativas.
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.
5. En la pestaña **General**, seleccionar la casilla de verificación **Catalogo global**.

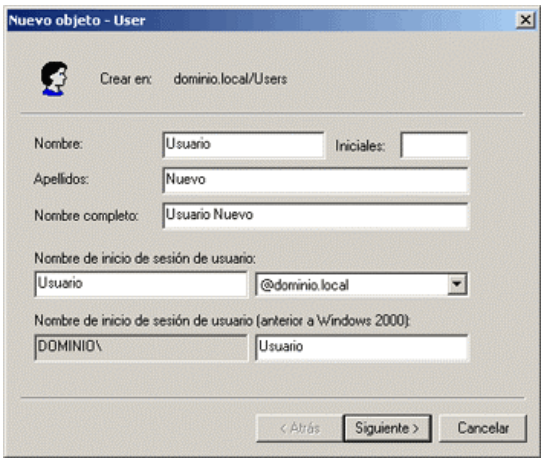
Mientras la empresa opere en modo mixto (esto es, que haya otros controladores de dominio además de los controladores de dominio Windows 2000), hay que tener al menos un servidor de Catalogo global por dominio. Una vez que se hayan actualizado todos los controladores de dominio a Windows 2000, se puede cambiar el dominio a modo nativo.

7.5.-Usuarios Globales. Copiar Cuentas de Usuario

Esquema General a seguir para copiar cuentas de usuario.

- Copiar cuentas de usuario:
  - Administrador de usuarios: seleccionar usuario | Usuario | Copiar | modificar datos | Agregar.
  - Crear una plantilla:

- Administrador de Usuarios | Usuario | Nuevo Usuario | introducir datos –desactivar la cuenta- | Agregar. Ahora podemos copiar.



Para copiar una cuenta de usuario hay que abrir "Usuarios y equipos de Active Directory" y entrar el la carpeta de la cuenta de usuario que deseemos copiar.

Sobre ese usuario, pulsando el botón derecho del ratón seleccionaremos la opción COPIAR.

Seguidamente hay que pulsar el botón AGREGAR y crear una nueva plantilla como se indica en el esquema de arriba.

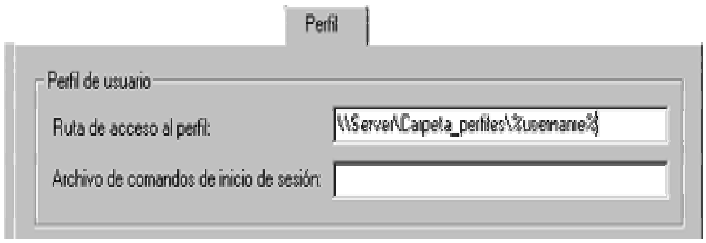
En Nombre de inicio de sesión de usuario, escriba el nombre con el que el usuario iniciará una sesión y, en la lista, haga clic en el sufijo UPN que se debe anexar al nombre de inicio de sesión de usuario, seguido del símbolo arroba (@).

Si el usuario va a utilizar un nombre diferente para iniciar una sesión en equipos donde se ejecuta Windows NT, Windows 98 o Windows 95, cambie el nombre de inicio de sesión de usuario que aparece en Nombre de inicio de sesión de usuario (anterior a Windows 2000) por el otro nombre.

Pulsando el botón siguiente nos aparecerá el formulario donde introducir la contraseña y Confirmar la misma y seleccionaremos las opciones de contraseña que desee.

Perfiles de Usuario: Móviles y Obligatorios

Perfil de usuario móvil. Los perfiles de usuario móviles los crea el administrador del sistema y se almacenan en un servidor. Este perfil está disponible siempre que el usuario inicie una sesión en cualquier equipo de la red. Los cambios efectuados en un perfil de usuario móvil se guardan en el servidor.



El funcionamiento es: se asigna una ubicación de un servidor para perfiles de usuario y se crea una carpeta compartida con los usuarios que tengan perfiles móviles. Se introduce una ruta de acceso a esa carpeta en la ventana propiedades de los usuarios. La siguiente vez que el usuario inicie sesión en un equipo, el perfil del servidor se descarga al equipo local. Cuando el usuario cierra la sesión, el perfil se almacena tanto localmente como en la ubicación de la ruta de acceso al perfil del usuario. La especificación de la ruta de acceso al perfil del usuario es todo

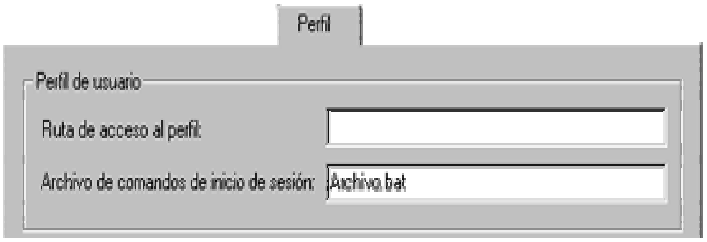
lo que hace falta para convertir un perfil local en un perfil móvil, disponible en cualquier parte del dominio.

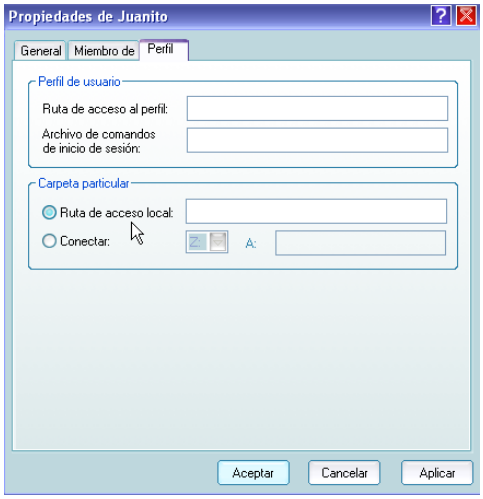
Para configurar un perfil móvil simplemente hay que asignar una ubicación en un servidor y completar los siguientes pasos:

Crear una carpeta compartida en el servidor para los perfiles.

En la pestaña Perfil de la ventana Propiedades de la cuenta de usuario hay que proporcionar una ruta de acceso a la carpeta compartida, como:

\\nombre_del_servidor\carpeta_de_perfiles_compartida\%username%.





Perfil de usuario obligatorio. Los perfiles de usuario obligatorios son perfiles móviles que se utilizan para especificar configuraciones particulares de usuarios o grupos de usuarios. Sólo los administradores del sistema pueden realizar cambios en los perfiles de usuario obligatorios.

Si se va a realizar todo el trabajo de asignar perfiles personalizados, indudablemente se deseara hacer que esos perfiles sean obligatorios. Un perfil obligatorio se puede asignar a múltiples usuarios. Cuando se modifica un perfil obligatorio, el cambio se realiza en los entornos de todos los usuarios a los cuales se haya asignado el perfil obligatorio. Para convertir un perfil en un perfil obligatorio, se debe renombrar el archivo oculto Ntuser.dat a Ntuser.man.

Perfil Movil:	NTUSER.DAT
Perfil Obligatorio:	NTUSER.MAN

Archivo de Comando de Inicio de Sesión

Esta secuencia de comandos se ejecuta cuando el usuario local inicia sesión en el equipo localmente, pero no se ejecuta cuando lo hace en el dominio.

Para completar este procedimiento, debe iniciar sesión como administrador o como miembro del grupo Administradores. Si el equipo está conectado a una red, la configuración de la directiva de red también afectará a la capacidad de completar este procedimiento.

Para asignar una secuencia de comandos a un perfil de usuario, siga estos pasos:

1. Haga clic en **Inicio** y después en **Panel de control**.
2. Haga doble clic en **Herramientas administrativas** y, después, haga doble clic en **Administración de equipos**.
3. En el árbol de consola, expanda **Usuarios y grupos locales** y, a continuación, haga clic en **Usuarios**.
4. Haga clic en la cuenta de usuario con la que desea trabajar.
5. Haga clic en **Acción** y después en **Propiedades**.
6. Haga clic en la ficha **Perfil** y, a continuación, escriba el nombre de archivo y la ruta de la secuencia de comandos en **Archivo de comandos de inicio de sesión**.
7. Haga clic en **Aplicar** y, después, haga clic en **Aceptar**.

Windows 2000 siempre busca las secuencia de comandos de inicio de sesión en el mismo lugar: en el controlador de dominio de autentificación en la ruta de acceso %SystemRoot%\SYSVOL\sysvol\nombre_del_ dominio. Las secuencias de comandos de esta carpeta se pueden introducir en la ruta de acceso Archivo de comandos de inicio de sesión solo con el nombre.

Las variables de secuencias de comando de inicio de sesión son:

%homedrive%: Letra de la unidad de disco que contiene el directorio principal del usuario en la estación de trabajo local del usuario.
%homepath%: Ruta de acceso completa al directorio principal del usuario.
%os%: Sistema operativo del usuario.
%processor_architecture%: Tipo de procesador de la estación de trabajo del usuario.
%processor_level%: Nivel de procesador de la estación de trabajo del usuario.
%userdomain%: Dominio donde esta definida la cuenta del usuario.
%username%: Nombre del usuario de la cuenta.

7.5.3.-La Ficha Perfil

En las instalaciones limpias de Windows 2000, el perfil de usuario local se almacena bajo el nombre del usuario en la carpeta

%userprofile%\Documents and Settings

Si el sistema ha sido actualizado a Windows 2000, el perfil de usuario local se almacena bajo el nombre del usuario en la carpeta

%systemroot%\perfiles

Cuando para un usuario no existe un perfil de usuario móvil preconfigurado en el servidor, la primera vez que el usuario inicia una sesión en un equipo, se crea una carpeta de perfil de usuario para dicho usuario en la carpeta Documents and Settings. A continuación, el contenido de Usuario predeterminado se copia en la nueva carpeta de perfil de usuario. El perfil de usuario, junto con las configuraciones de los grupos de programas comunes de la carpeta All Users (dentro del directorio Documents and Settings), crea el escritorio del usuario. Cuando el usuario termina la sesión, todos los cambios realizados durante la sesión sobre la configuración predeterminada se guardan en la nueva carpeta de perfil de usuario. El perfil de usuario de Usuario predeterminado no se cambia.

Si el usuario tiene una cuenta de usuario en el equipo local además de una o varias cuentas de usuario de dominio, el perfil de usuario local es diferente para cada cuenta, puesto que se generan perfiles de usuario diferentes para cada usuario que inicia una sesión. Cuando el usuario termina la sesión, las configuraciones modificadas sólo se guardan en un perfil de usuario, en el de la cuenta con la que el usuario haya iniciado la sesión.

Para crear un perfil móvil u obligatorio deberemos dar los siguientes pasos:

Abriremos Administración de equipos dentro las Herramientas Administrativas del panel del control.

En el árbol de la consola, haga clic en Usuarios.

Haga clic con el botón secundario del *mouse* (ratón) en la cuenta de usuario que desee y, después, haga clic en Propiedades.

En la ficha Perfil, en Ruta de acceso al perfil, escriba la ruta de acceso al recurso donde se guardará el perfil.

En el caso de una ruta de acceso de red, utilice este formato:

\\nombreServidor\nombreCarpetaPerfiles\nombrePerfilUsuario

Crear un Perfil Preconfigurado para cada Usuario

El primer paso para crear un perfil preconfigurado para cada usuario es crear un perfil como se crean normalmente y como se ha indicado en puntos anteriores de este trabajo.

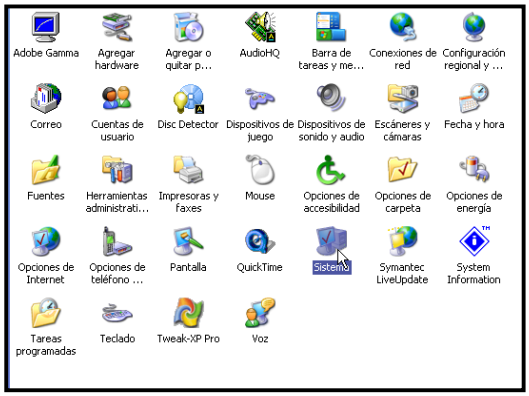
Inicie sesión en el equipo como administrador y cree una cuenta de usuario local.

Cierre la sesión como administrador e inicie sesión en el equipo mediante la cuenta de usuario local recién creada.

Tenga en cuenta que se producirán problemas con los permisos si el perfil de usuario personalizado se crea al iniciar sesión como administrador.

Personalice el perfil en consecuencia. Por ejemplo, instale las impresoras y asigne las unidades necesarias.

Cierre sesión como usuario local y vuelva a iniciar sesión como administrador.



Como varios de los archivos del perfil son ocultos y deben copiarse al nuevo perfil de usuario predeterminado personalizado, active la opción **Mostrar todos los archivos y carpetas ocultos**:

Haga doble clic en **Mi PC**, haga clic en **Herramientas** y, después, haga clic en **Opciones de carpeta**.

En la ficha **Ver**, bajo **Configuración avanzada** , haga clic en **Mostrar todos los archivos y carpetas ocultos** y, después, haga clic en **Aceptar**.

En este punto es cuando una vez hayamos entrado con como Administrador, nos dirigimos al panel de control y realizamos la siguientes operaciones:

Reemplace el perfil de usuario predeterminado actual por el perfil de usuario predeterminado personalizado:

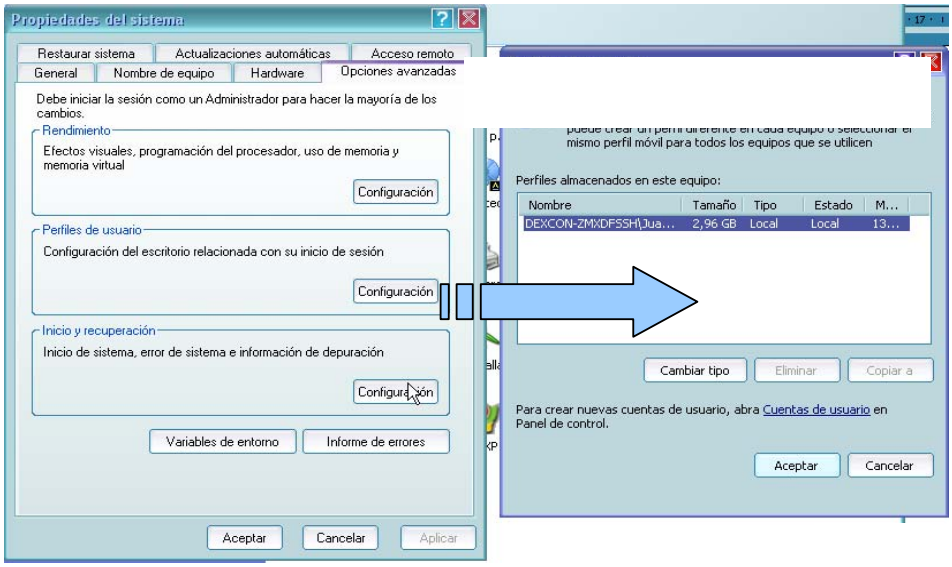
Haga clic en **Inicio**, seleccione **Configuración** y, a continuación, haga clic en **Panel de control**.

Haga doble clic en **Sistema**.

En la ficha **Perfiles de usuario**, haga clic en el perfil de usuario recién creado y, después, haga clic en **Copiar a**.

En el cuadro de diálogo **Copiar a**, bajo **Copiar perfil en** , haga clic en **Examinar**, haga clic en la carpeta **\Documents and Settings\Default User** y, después, haga clic en **Aceptar**.

En **Está permitido usar** , haga clic en **Cambiar**, **Todos**, **Aceptar**.



7.6.-Grupos. Ambito de un Grupo

Además de gestionar cuentas de usuario, Windows 2000 es capaz de gestionar grupos, para conceder permisos a usuarios similares y para simplificar la administración de las cuentas.

Si un usuario es miembro de un grupo puede acceder a un recurso, si este esta permitido para el grupo.

Los dominios de Active Directory Pueden tener grupos con el mismo nombre, estos se identifican habitualmente como:

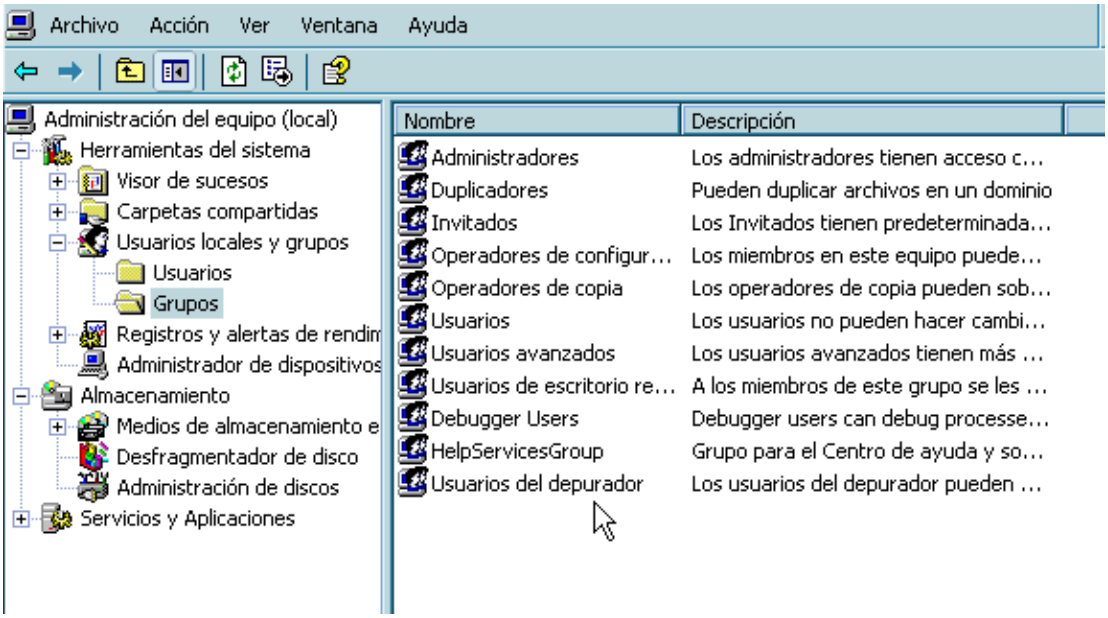
DOMINIO\NombreDeGrupo

Hay tres tipos de grupos en Windows 2000:

Grupos locales: son grupos que se definen en un equipo local. Para crearlos usar la utilidad Usuarios y grupos locales.

Grupos de seguridad: son grupos con descriptores de seguridad asociados a ellos. Se configuran en Usuarios y equipos de Active Directory.

Grupos de distribución: son grupos que se utilizan para las lista de distribuciónde correo electrónico. No pueden tener descriptores de seguridad asociados. Se configuran en Usuarios y equipos de Active Directory.



Ámbitos de un Grupo:

A un grupo con ámbito global los permisos se pueden conceder para recursos ubicados en cualquier dominio. Sin embargo, los miembros sólo pueden proceder del dominio en el que se crea el grupo, y en ese sentido no es global. Los grupos globales son adecuados para objetos de directorio que requieren mantenimiento frecuente, como cuentas de usuario y grupo.

Pueden ser miembros de:

- Grupos universales o locales de dominio en cualquier dominio.
- Pueden contener los siguientes miembros:
  - Otros grupos globales en el mismo dominio.
  - Cuentas individuales del mismo dominio.

Un grupo de seguridad universal puede tener miembros procedentes de cualquier dominio y se le pueden asignar permisos para recursos de cualquier dominio. El ámbito universal sólo esta disponible en dominios que se ejecuten en modo nativo. Los grupos universales pueden tener los siguientes miembros:

Otros grupos universales.

Grupos globales.

Cuentas individuales.

Grupos globales predefinidos

Los grupos globales predefinidos se crean para englobar tipos de cuentas comunes. De forma predeterminada, estos grupos no tiene derechos heredados; un administrador debe

asignar todos los derechos del grupo. Sin embargo, algunos miembros se añaden automáticamente a estos grupos, y se pueden añadir como miembros basándose en los derechos y permisos asignados a los grupos. Los derechos se pueden asignar directamente a los grupos o añadiendo los grupos globales predefinidos a grupos locales de dominio.

Grupos globales predefinidos usados más frecuentemente

- **Administración de empresas:** Este grupo es para usuarios que tengan derechos administrativos en toda la red. Administración de empresas es automáticamente un miembro del grupo local de dominio Administradores en el dominio en el que se creo. Será necesario añadirlo al grupo local de dominio Administradores de otros dominios.
- **Admins. del dominio:** Este grupo es automáticamente un miembro del grupo local de dominio Administradores, por lo que los miembros de Admins. del dominio pueden realizar tareas administrativas en cualquier equipo del dominio. La cuenta Administrador es un miembro de este grupo de forma predeterminada.
- **Controladores del dominio:** Todos los controladores de dominio del dominio con miembros.
- **Equipos del dominio**: Son miembros todos los controladores y estaciones de trabajo del dominio.
- **Invitados del dominio:** La cuenta Invitado es un miembro de forma predeterminada. Este grupo es automáticamente un miembro del grupo local de dominio Invitados.
- **Propietarios del creador de directivas de grupo:** Sus miembros pueden crear y modificar la directiva de grupo del dominio.
- **Usuarios del dominio:** Todos los usuarios del dominio y la cuenta Administrador son miembros. El grupo Usuarios del dominio es automáticamente un miembro del grupo local de dominio usuarios.

Si se tienen usuarios que deberían tener menos derechos y/o permisos que los de un usuario típico, hay que añadir esos usuarios a Invitados de dominio y eliminarlos de Usuarios del dominio.

Grupos locales predefinidos

Los servidores miembro, los servidores independientes y los equipos que ejecutan Windows 2000 Profesional tienen grupos locales predefinidos que otorgan derechos para realizar tareas en una única maquina.

Si se desea que los miembros del grupo Usuarios del dominio no tengan acceso a una estación de trabajo o servidor miembro en particular, hay que eliminar Usuarios del dominio del grupo local Usuarios de ese equipo. De forma similar, si no se desea que los miembros de

Admins. del dominio administren una estación de trabajo o un servidor miembro en particular, hay que eliminar Admins. del dominio del grupo local Administradores.

Grupos locales predefinidos:

- **Administradores:** Sus miembros pueden realizar todas las tareas administrativas en el equipo. La cuenta predefinida Administrador que se crea cuando se instala el sistema operativo es un miembro del grupo. Cuando un servidor independiente o un equipo que ejecuta Windows 2000 Profesional se une a un dominio, el grupo Admins. del dominio se hace parte de este grupo.

- **Duplicadores:** No se deben añadir cuentas de usuario de usuarios reales a este grupo. Si es necesario, se puede añadir una cuenta de usuario "ficticia" a este grupo para permitir iniciar sesión en los servicios Replicador de un controlador de dominio para administrar la réplica de archivos y directorios.

- **Invitados:** Sus miembros solo pueden realizar tareas para las cuales el administrador haya concedido permisos. Los miembros solo pueden utilizar aquellos recursos para los que un administrador haya concedido permisos específicamente.

- **Operadores de copia:** Sus miembros pueden iniciar sesión en el equipo, hacer copia de seguridad y recuperar la información del equipo y apagar el equipo. Los miembros no pueden cambiar la configuración de seguridad. No hay miembros predeterminados en el grupo.

- **Usuarios:** Los miembros de este grupo pueden iniciar sesión en el equipo, acceder a la red, almacenar documentos y apagar el equipo. Los miembros no pueden instalar programas o hacer cambios en el sistema. Cuando un servidor miembro o una maquina Windows 2000 Profesional se une a un dominio, el grupo Usuarios del dominio se añade a este grupo.

- **Usuarios avanzados:** Sus miembros pueden crear y modificar cuentas de usuario e instalar programas en el equipo local pero no pueden ver los archivos de otros usuarios.

Grupos locales de dominio predefinidos

Los grupos locales de dominio predefinidos de Windows 2000 proporcionan a los usuarios derechos y permisos para realizar tareas en controladores de dominio y en el Active Directory. Los grupos locales de dominio tienen derechos y permisos predefinidos que están concedidos a los usuarios y a los grupos globales que se añaden como miembros.

Grupos locales de dominio predefinidos usados más frecuentemente

- **Administradores:** Sus miembros tienen concedido automáticamente cualquier derecho o permiso de todos los controladores de dominio y del propio dominio. La cuenta Administrador, el grupo Administración de empresas y el grupo Admins. del dominio son miembros.

- **Invitados:** Sus miembros solo pueden realizar tareas para las cuales el administrador haya concedido permisos. Los miembros solo pueden utilizar aquellos recursos para los que un administrador haya concedido permisos específicamente. Los grupos Usuarios invitados a Invitados de dominio son miembros de forma predeterminada.

- **Operadores de copia:** Sus miembros pueden hacer copia de seguridad y recuperar información en todos los controladores de dominio utilizando Copia de seguridad de Windows 2000.

- **Operadores de cuentas:** Sus miembros pueden crear, eliminar y gestionar cuentas y grupo de usuarios. Los miembros no pueden modificar el grupo Administradores o cualquiera de los grupos Operadores.

- **Operadores de impresión:** Sus miembros pueden gestionar todos los aspectos de la operación y configuración de impresoras en el dominio.

- **Operadores de servidores:** Sus miembros pueden realizar la mayoría de las tareas administrativas en los controladores de dominio, excepto la manipulación de las opciones de seguridad.

- **Usuarios:** Sus miembros pueden iniciar sesión en el equipo, acceder a la red, almacenar documentos y apagar el equipo. Los miembros no pueden instalar programas o hacer cambios en el sistema. El grupo Usuarios del dominio es miembro de este grupo de forma predeterminada.

7.7.-Equipos. Cuentas de Equipo

Todos los equipos donde se ejecuta Windows 2000 o Windows NT que se unen a un dominio tienen una cuenta de equipo. Las cuentas de equipo son similares a las cuentas de usuario y ofrecen un medio para autenticar y auditar el acceso a la red de los equipos y el acceso a los recursos del dominio. Cada equipo conectado a la red debería tener su propia cuenta de equipo única. Las cuentas de equipo también se crean mediante Usuarios y equipos de Active Directory.

La forma más fácil de crear un cuenta de equipo es iniciar la sesión en un equipo y unirse a un dominio. Al hacerlo se crea automáticamente una cuenta de equipo y se ubica en la carpeta Equipos o en Controladores de Dominio.

Cada cuenta de equipo creada en Active Directory tiene un nombre completo relativo, un nombre de equipo de Windows 2000 (nombre de cuenta de administración de seguridad), un sufijo DNS principal, un nombre de host y un nombre principal de servicio. El administrador escribe el nombre del equipo cuando crea la cuenta del equipo. Este nombre de equipo se utiliza como nombre completo relativo LDAP.

Active Directory sugiere un nombre de inicio de sesión de usuario de sistema anterior a Windows 2000 a partir de los primeros 15 bytes del nombre completo relativo. El

administrador puede cambiar el nombre de inicio de sesión de sistema anterior a Windows 2000 siempre que lo desee.

De forma predeterminada, el sufijo DNS adopta el nombre DNS completo del dominio al que se une el equipo. El nombre de host DNS se crea a partir de los 15 primeros caracteres del nombre completo relativo y el sufijo DNS principal. Por ejemplo, el nombre de host DNS del equipo que se une al dominio *miDominio.microsoft.com* y que tiene el nombre completo relativo *CN=MiPC1234567890*, sería *miPC12345.miDominio.microsoft.com*.

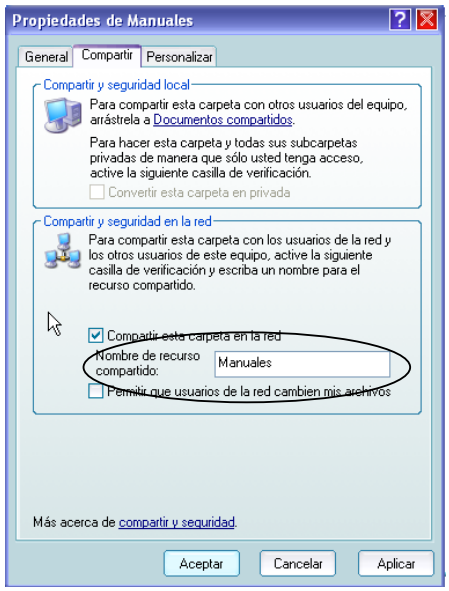
7.8.-Directorios. Permisos a Carpetas Compartidas

Se puede compartir un directorio en el sistema para que varios usuarios puedan acceder por igual a él. Pero también es necesario establecer unas medidas de seguridad para evitar que usuarios no deseados accedan al directorio compartido.

En las propiedades de la carpeta en compartir vamos a la opción permitir y decidimos cuantos usuarios a la vez pueden visualizar esa carpeta.

Se pueden dar diversos tipos de acceso a las carpetas compartidas:

- Sin acceso (NO COMPARTIDO): no se otorga ningún permiso sobre el directorio compartido.
- Leer: los usuarios pueden ver los nombres de archivos y subcarpetas, tener acceso a las subcarpetas, leer datos y atributos de los archivos y ejecutar archivos de programa..

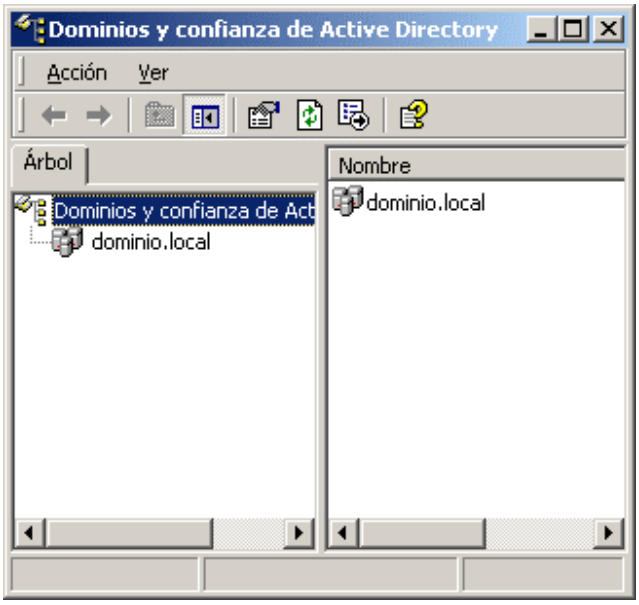


- Cambiar: los usuarios tienen permiso de leer y capacidad adicional para crear archivos y subcarpetas, modificar archivos, cambiar atributos en archivos y subcarpetas, eliminar archivos y subcarpetas.

- Control Total: los usuarios tienen los permisos de Leer y Cambiar, y en los volúmenes NTFS además pueden cambiar permisos de archivos y carpetas y tomar posesión de archivos y carpetas.

Mediante la carpeta Herramientas Administrativas del panel de control podemos llegar a situarnos en la opción de Carpetas compartidas, desde donde podremos hacer las siguientes operaciones:

Crear, ver y establecer permisos en recursos compartidos.



Ver una lista de todos los usuarios conectados al equipo a través de una red y desconectar alguno de ellos o todos.

Ver una lista de los archivos abiertos por usuarios remotos y cerrar alguno de ellos o todos.

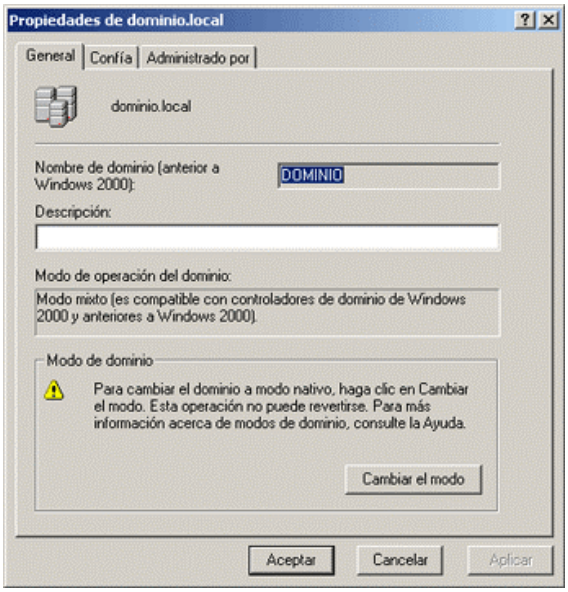
7.9.-Establecimiento de Permisos de Toma de Posesión

Para la configuración de permisos de toma de posesión sobre archivos o directorios, en la ficha de seguridad del directorio o archivo hay que habilitar permiso "Toma de posesión".

Para lo cual haremos lo siguiente:

Clic con el botón derecho en el directorio compartido que se va a administrar y seleccionar Propiedades.

Clic en ficha de Permisos de recursos compartidos.



Dar el permiso de toma de posesión.

Clic en Aceptar.

Se pueden dar permisos de toma de posesión a usuarios pero el administrador no puede dárselos a nadie, en cambio puede tomar posesión cuando quiera de una carpeta. Por defecto el propietario, el usuario que toma posesión, es aquel que crea el directorio o archivo.

7.10.-Dominios y confianzas de Active Directory

Los *Dominios y confianzas de Active*

Directory de Windows 2000 es un complemento MMC que se puede utilizar para consultar un árbol que contiene todos los dominios del bosque. Con este complemento se pueden administrar las relaciones de confianza entre los dominios, cambiar el modo del dominio y configurar los sufijos del nombre principal de usuario (UPN, User Principal Name) para el bosque. Dominios y confianzas de Active Directory también proporciona acceso a Usuarios y equipos de Active Directory, que se puede utilizar para consultar y modificar las propiedades de los objetos individuales.

Inicio de Dominios y confianzas de Active Directory

Windows 2000 Server añade el complemento Administrador de Dominios y confianzas de Active Directory al menú Inicio de forma predeterminada, por lo que después de iniciar sesión utilizando una cuenta con privilegios administrativos se puede ejecutar la utilidad seleccionando **Dominios y confianzas de Active Directory** desde **Herramientas administrativas** en el grupo Programas del menú Inicio. El archivo del complemento MMC se llama **Domain.msc**, por lo que también se puede ejecutar el administrador desde el cuadro de dialogo Ejecutar ejecutando ese nombre de archivo.

Cuando se carga el Administrador de **Dominios y confianzas de Active Directory**, el árbol de la consola (a la izquierda) muestra todos los dominios del bosque como un árbol que se expande, partiendo de una raíz etiquetada como Dominios y confianza de Active Directory. El panel de resultados (a la derecha) muestra los secundarios del dominio seleccionado actualmente o, si se selecciona la raíz, los dominios raíz de todos los árboles del bosque. Las funciones que proporciona Dominios y confianzas de Active Directory están todas accesibles desde los menús Acción que se originan pulsando un nombre de dominio o el objeto raíz, además de dentro de la ventana Propiedades de un dominio.

Cambio del modo del dominio

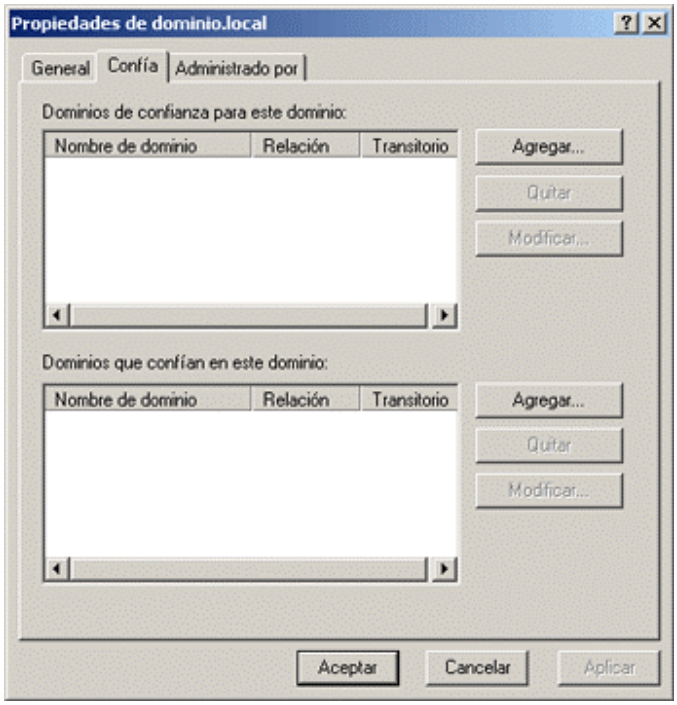
Desde Dominios y confianzas de Active Directory, cuando se abre la ventana Propiedades de un dominio, la pestaña General muestra el nombre NetBIOS con el cual conocen los clientes de nivel inferior al dominio y permite especificar una descripción para ese dominio. Esta pestaña también muestra el modo de operación actual del dominio y permite cambiarlo.

De forma predeterminada, los controladores de dominio recién instalados operan en modo mixto, lo que significa que se pueden utilizar BDC Windows NT como controladores de dominio en un dominio Windows 2000. De esta forma, se puede actualizar un dominio Windows NT existente a Windows 2000 de forma gradual actualizando primero el PDC Windows NT a Windows 2000. después se puede utilizar Active Directory para almacenar información sobre el dominio y modificar el directorio utilizando los complementos de Active Directory incluidos en Windows 2000 Server.

Cuando Windows 2000 Server opera en modo mixto, los BDCs Windows NT son controladores de dominio completamente funcionales en el dominio Active Directory, capaces de realizar replica con múltiples maestros al igual que los controladores de dominio Windows 2000. El único inconveniente de utilizar el modo mixto es que no se pueden aprovechar las

ventajas de las características avanzadas de agrupación de Windows 2000, como la posibilidad de anidar grupos y crear grupos con miembros en dominios diferentes.

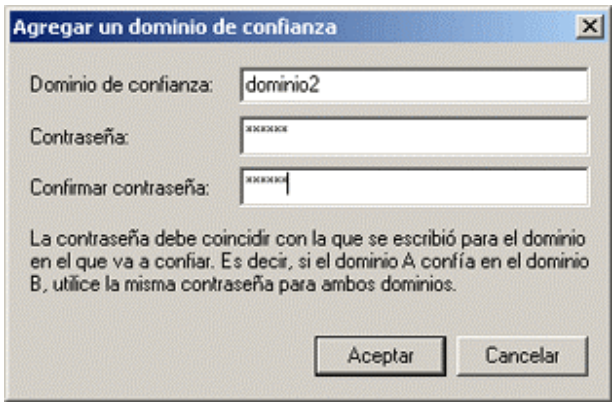
Una vez que se ha completado la actualización a Windows 2000 de todos los BDC Windows NT del dominio, se puede cambiar el equipo a modo nativo, lo que activa estas capacidades de agrupación. Sin embargo, una vez que se ha cambiado el modo de operación del dominio de mixto a nativo, no se puede cambiar de nuevo sin reinstalar Active Directory. Hay que asegurarse de que no se necesitaran mas los controladores de dominio Windows NT de la red antes de hacer esta modificación.



El modo mixto se refiere únicamente a los controladores de dominio en un dominio particular. Después de cambiar a modo nativo, todavía se pueden utilizar controladores de dominio Windows NT en el mismo Árbol, siempre y cuando estén ubicados en diferentes dominios.

Gestión de las relaciones de confianza entre dominios

La relación de confianza entre dominios se gestiona desde la pestaña Confía de la ventana Propiedades de un dominio. Cuando se establece una relación de confianza entre dos dominios, los usuarios de un dominio pueden acceder a recursos ubicados en otro dominio en que se confíe. Un árbol de dominios Active Directory es una colección de dominios que no sólo comparten el mismo esquema, la configuración y el espacio de nombres, sino que también están conectados por medio de relaciones de confianza.



Windows 2000 soporta dos tipos de relaciones de confianza: las confianzas explicitas y de un sentido utilizadas por Windows NT, y las confianzas transitivas y jerárquicas proporcionadas por el protocolo de seguridad Kerberos en los dominios Active Directory. Las relaciones de confianza de Windows NT sólo funcionan en un sentido. Por ejemplo, el hecho de que el dominio A confié en los usuarios del dominio B no

implica que B confié en los usuarios de A automáticamente. Un administrador debe crear explícitamente las confianzas en ambos sentidos para lograr una relación mutua entre los dominios.

Active Directory crea automáticamente relaciones de confianza Kerberos en todos los dominios de un árbol; estas se aplican en ambos sentidos y son transitivas. Una relación de confianza transitiva es aquella que se propaga a través de la jerarquía del árbol. Por ejemplo, cuando un dominio A confía en un dominio B y un dominio B confía en un dominio C, entonces el dominio A confía en el dominio C. La creación de cada nuevo dominio en un árbol incluye el establecimiento de las relaciones de confianza con el resto de dominios del árbol, lo que permite a los usuarios acceder a recursos en cualquiera de los dominios del árbol (asumiendo que tienen los permisos apropiados) sin que un administrador tenga que configurarlo manualmente.

Para proporcionar acceso al dominio a usuarios de otro árbol o para conceder acceso a otro árbol a los usuarios del dominio, se pueden establecer relaciones de confianza manualmente pulsando uno de los botones **Agregar** de la pestaña **Confía** y especificando el **nombre NetBIOS** de un dominio. Estas relaciones son en un solo sentido; hay que establecer una confianza para cada dominio para crear una confianza bidireccional. Dependiendo de la naturaleza del dominio que confía o en el que se confía, la relación podrá o no ser transitiva. Se puede establecer una relación de confianza transitiva con dominios Windows 2000 en otro árbol, pero las relaciones con dominios Windows NT no pueden ser transitivas.

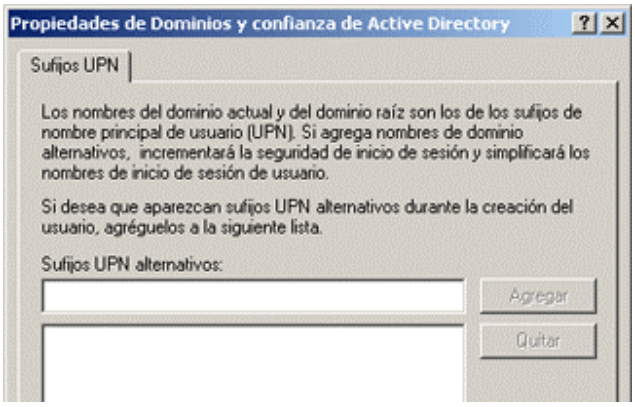
Para establecer una relación de confianza con otro dominio, hay que especificar el nombre del dominio en el cuadro de dialogo Agregar un dominio de confianza y proporcionar una contraseña. Para completar el proceso, un administrador del otro dominio debe especificar el nombre de este dominio en el cuadro de dialogo Agregar un dominio que confía y proporcionar la misma contraseña. Ambos dominios deben dar su aprobación antes de que los sistemas puedan establecer la relación de confianza.

Especificación del administrador del dominio

La tercera pestaña de la ventana Propiedades de un dominio, identifica al individuo que es el administrador designado para el dominio. Esta pestaña proporciona información de contacto sobre el administrador derivada de la cuenta de usuario asociada en Active Directory. Se puede cambiar el administrador pulsando el botón Cambiar y seleccionando otra cuenta de usuario desde la pantalla de Active Directory que se muestra.

Configuración de los sufijos de nombre principal de usuario en un bosque

Un UPN es un nombre simplificado que los usuarios pueden proporcionar cuando inician sesión en Active Directory. El nombre utiliza el formato estándar de direcciones de correo electrónico que consiste en un nombre de usuario prefijo y un nombre de dominio sufijo, separados por un signo @, como se define en la RFC 822 (por ejemplo, usuario@dominio.com). Los UPNs proporcionan a los usuarios de la red un formato de nombre de inicio de sesión unificado que los aísla de la jerarquía de dominios de Active Directory y de la necesidad de especificar el complejo nombre LDAP para sus objetos usuario cuando inician sesión.



De forma predeterminada, el sufijo del UPN de los usuarios de un bosque en particular es el nombre del primer dominio creado en el primer árbol del bosque, también llamado el hombre DNS del bosque. Por medio del Administrador de Dominios y confianzas de Active Directory se pueden especificar sufijos UPN adicionales que los usuarios pueden emplear en lugar del hombre DNS del bosque cuando inicien sesión. Para hacer esto, hay que seleccionar el objeto raíz en el árbol de la consola de la pantalla principal de Dominios y confianzas de Active Directory, y escoger Propiedades en el menú Acción. En la pestaña Sufijos UPN, hay que pulsar el botón Agregar para especificar sufijos adicionales. Estos sufijos se aplican en todo el bosque y están disponibles para cualquier usuario de cualquier dominio de cualquier árbol de ese bosque.

Gestión de los dominios

El complemento Dominios y confianzas de Active Directory también proporciona acceso al complemento Usuarios y equipos de Active Directory que se utiliza para consultar y modificar los objetos de un dominio y sus propiedades. Cuando se selecciona un dominio en el árbol de la consola de la pantalla principal y se escoge Administrar en el menú Acción, la MMC

abre el complemento Usuarios y equipos de Active Directory con el foco en el dominio seleccionado.

7.11.-Tipos de objetos de Active Directory

Los objetos de la pantalla Usuarios y equipos de Active Directory representan tanto entidades físicas, como equipos y usuarios, como las entidades lógicas, como grupos y unidades organizativas.

Modificando el esquema que controla la estructura del servicio de directorio, se pueden crear nuevos tipos de objetos en Active Directory y modificar los atributos de los tipos existentes.

Modo normal y modo avanzado

De forma predeterminada, la pantalla Usuarios y equipos de Active Directory opera en modo normal. El modo normal solo muestra los objetos a los que los administradores accederán con mayor probabilidad durante una sesión de mantenimiento de Active Directory típica. Esto incluye las unidades organizativas que contienen los usuarios y grupos predefinidos creados durante la instalación de Active Directory y todos los objetos creados por los administradores después de la instalación. El modo normal también oculta ciertas pestañas de la ventana Propiedades de un objeto, incluyendo la pestaña Objeto y la pestaña Seguridad que se pueden utilizar para establecer permisos para el objeto.

Dominio: Objeto raíz de la pantalla Usuarios y equipos de Active Directory; identifica el dominio que está administrando actualmente el administrador.

Unidad organizativa: Objeto contenedor utilizado para crear agrupaciones lógicas de objetos equipo, usuario y grupo.

Usuario: Representa un usuario de la red y funciona como un almacén de información de identificación y autenticación.

Equipo: Representa un equipo de la red y proporciona la cuenta de maquina necesaria para que el sistema inicie sesión en el dominio.

Contacto: Representa un usuario externo al dominio para propósitos específicos como envío de correo electrónico; no proporciona las credenciales necesarias para iniciar sesión en el dominio.

Grupo: Objeto contenedor que representa una agrupación lógica de usuarios, equipos a otros grupos (o los tres) que es independiente de la estructura del árbol de Active Directory. Los grupos pueden contener objetos de diferentes unidades organizativas y dominios.

Carpeta compartida: Proporciona acceso de red, basado en Active Directory, a una carpeta compartida en un sistema Windows 2000.

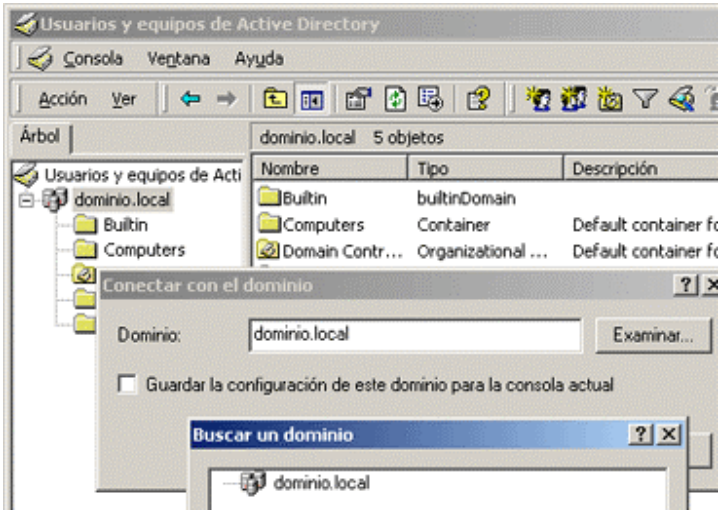
Impresora compartida: Proporciona acceso de red, basado en Active Directory, a una impresora compartida en un sistema Windows 2000.

Sin embargo, cuando se escoge Características avanzadas en el menú Ver del administrador, la pantalla cambia para incluir todos los objetos Active Directory del sistema que representan directivas, registros DNS y otros elementos del servicio de directorio, además del contenedor LostAndFound.

Desde esta interfaz se puede consultar información sobre los objetos del sistema y controlar el acceso a ellos modificando los permisos asociados. Como el acceso a estos objetos no se requiere con frecuencia, se puede impedir que aparezcan dejando el administrador en modo normal. Sin embargo, cuando haya que modificar los permisos de los objetos estándar como unidades organizativas, usuarios y grupos, habrá que activar las Características avanzadas para acceder a la pestaña Seguridad de la ventana Propiedades de un objeto.

Cambio de dominio

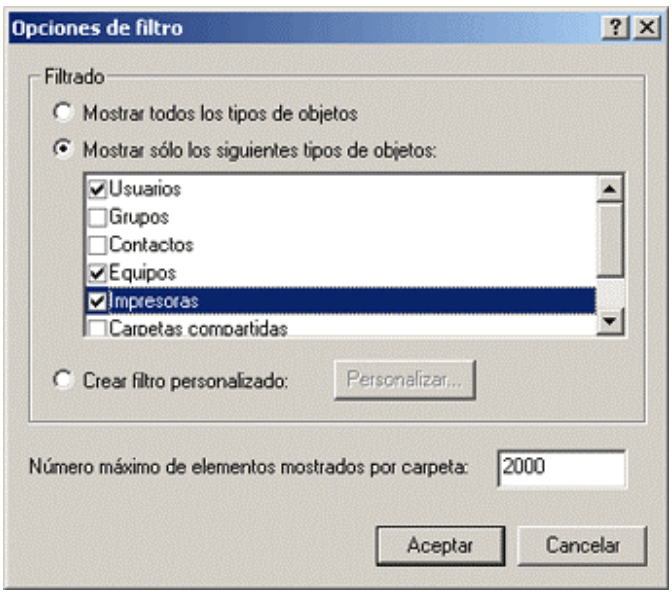
Se puede utilizar el complemento Usuarios y equipos de Active Directory para administrar cualquier dominio de la red. Para cambiar el dominio que se muestra en el administrador, hay que resaltar la raíz o el objeto dominio en el árbol de la consola y escoger Conectar con el dominio en el menú Acción. Esto muestra el cuadro de diálogo Conectar con el dominio, donde se puede introducir el nombre del dominio o buscar otro dominio.



En el menú **Acción** también se puede escoger **Conectar** con el controlador de dominio para acceder al dominio seleccionado utilizando un controlador de dominio especifico de la red. A menos que los controladores de dominio no estén sincronizados, la información debería ser la misma en todas las replicas, pero algunas veces puede ser útil seleccionar un controlador de dominio en una ubicación diferente para evitar una lenta o cara conexión WAN.

Filtros para simplificar la visualización

Cuando se empieza a poblar Active Directory con nuevos objetos, puede crecer rápidamente a un tamaño difícil de manejar. El mero número de objetos en la pantalla puede dificultar la localización del objeto especifico que se necesita. Para evitar que se muestren temporalmente los objetos que no es necesario ver, se puede aplicar un filtro al complemento

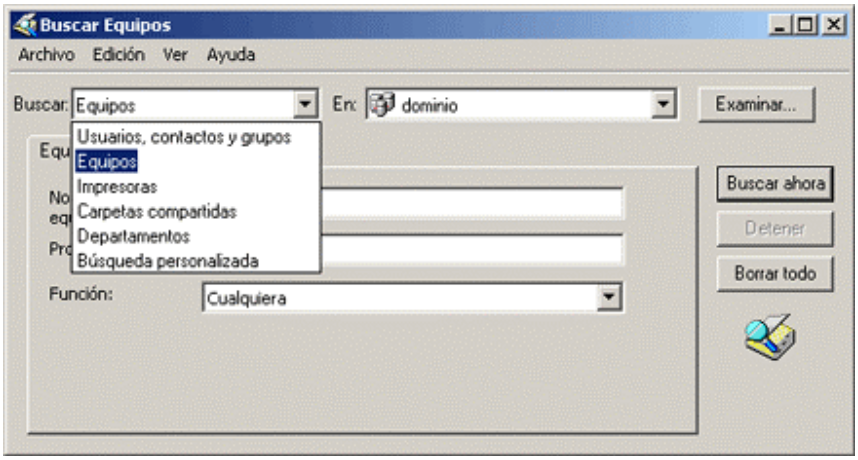


Usuarios y equipos de Active Directory basándose en los tipos de objetos o basándose en el contenido de atributos de objetos específicos.

Cuando se escoge Opciones de filtro desde el menú Ver, aparece el cuadro de diálogo Opciones de filtro. Aquí se puede optar por mostrar todos los tipos de objetos, seleccionar tipos de objetos específicos a mostrar o crear un filtro personalizado basándose en los atributos de los objetos.

Cuando se selecciona la opción Crear filtro personalizado y se pulsa el botón Personalizar, se muestra un cuadro de diálogo Buscar Búsqueda personalizada. En este cuadro de diálogo se puede seleccionar un tipo de objeto, escoger un atributo de ese objeto y especificar un valor completo o parcial para ese atributo.

Por ejemplo, se pueden mostrar solo los objetos usuario que tengan el valor Ventas en el atributo Departamento (como se muestra en la figura), o se puede optar por mostrar sólo los usuarios que tienen un código de área particular en el atributo Número de teléfono. Esto permite ajustar la mira rápidamente en los objetos que se necesitan utilizar sin tener que desplazarse a lo largo de una pantalla innecesariamente abarrotada.



Búsqueda de objetos

También se pueden buscar objetos específicos en todo Active Directory sin modificar lo que muestra el administrador. Si se selecciona el objeto dominio y se escoge Buscar en el menú Acción, se muestra el. cuadro de dialogo Buscar Usuarios, contactos y grupos, en el cual se puede especificar el tipo de objeto que se desea localizar, un dominio especifico o todo el directorio y el nombre y descripción del objeto.

El programa busca entonces en el CG que se creo automáticamente en el primer controlador del dominio para localizar el objeto deseado. El CG es un subconjunto de todo

Active Directory que solo contiene los atributos mas comúnmente utilizados, lo que facilita la búsqueda de un objeto especifico. Sin el CG, la tarea de buscar en una instalación Active Directory que incluye controladores de dominio en ubicaciones remotas podría requerir un extenso trafico WAN que es tan lento como caro.

A pesar de que Active Directory siempre crea el CG en el primer controlador de dominio de un dominio, se puede cambiar su ubicación predeterminada modificando la configuración NTDS en el complemento Sitios y servicios de Active Directory. También se pueden especificar atributos adicionales que han de almacenarse en el CG utilizando el complemento Esquema de Active Directory.

La pestaña Opciones avanzadas del cuadro de dialogo Buscar Usuarios, contactos y grupos utiliza la misma interfaz que la característica Filtro personalizado. De la misma forma, se pueden buscar objetos basándose en sus atributos. Si un atributo que se selecciona no es parte del CG, la búsqueda procederá inspeccionando el contenido real de los controladores de dominio de la red. En algunos casos, esto puede ralentizar considerablemente el proceso de búsqueda.

Mucha de la misma funcionalidad de búsqueda de objetos de Active Directory que se encuentra en el complemento Usuarios y equipos de Active Directory también esta disponible en la característica Buscar del menú Inicio.

Objetos predeterminados de Active Directory

Un dominio Active Directory recién creado contiene objetos unidades organizativas, equipos, usuarios y grupos que crea de forma predeterminada el Asistente para instalación de Active Directory. Estos objetos proporcionan acceso al sistema a varios niveles e incluyen grupos que permiten a los administradores delegar tareas de mantenimiento de la red especificas a otros. Incluso si no se espera utilizar esos objetos en el futuro, hay que utilizarlos para crear otros objetos con los permisos apropiados para la red.

Por ejemplo, aun si no se desea tener ningún usuario único con el control completo concedido a la cuenta de administrador, hay que iniciar sesión como administrador para poder crear los nuevos objetos usuario con los derechos y permisos deseados. Con Active Directory se pueden dejar partes de la estructura del directorio «huérfanas» si se modifica, se borra o se desactiva la cuenta de administrador sin haber creado primero otros objetos usuario o haberles concedido permisos equivalentes para las distintas partes del directorio.

Los objetos predeterminados creados en un dominio Active Directory, junto con sus funciones y sus ubicaciones en la jerarquía del dominio.

Objetos creados de forma predeterminada en un dominio Active Directory			
Nombre del objeto	**Tipo de objeto**	**ubicación**	**Función**

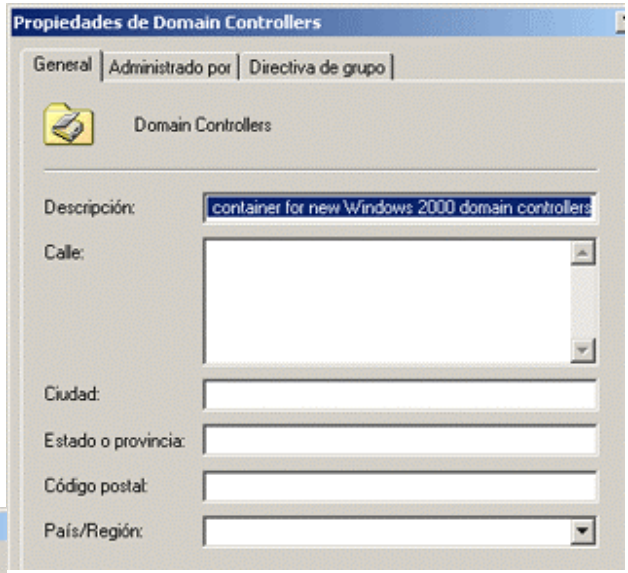
Builtin	builtinDomain	Dominio raíz	Contenedor predeterminado para los grupos que proporcionan acceso a las funciones de administración del servidor.
Computers	Contenedor	Dominio raíz	Contenedor predeterminado para cuentas de equipo actualizadas.
Users	Contenedor	Dominio raíz	Contenedor predeterminado para cuentas de usuario actualizadas.
Domain controllers	Unidad organizativa	Dominio raíz	Contenedor predeterminado para los nuevos controladores de dominio Windows 2000.
Opers. de cuentas	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden administrar las cuentas de usuario y de grupo del dominio.
Administradores	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden administrar completamente el equipo/dominio.
Operadores de copia	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden saltarse la seguridad de los archivos para hacer copia de seguridad de ellos.
Invitados	Grupo de seguridad. Integración local	Builtin	Usuarios que tienen concedido acceso de invitado al equipo/dominio.
Opers. de impresión	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden administrar las impresoras del dominio.
Duplicadores	Grupo de seguridad. Integración local	Builtin	Soporta la replica de archivos en un dominio.
Opers. de servidores	Grupo de seguridad. Integración local	Builtin	Sus miembros pueden administrar. servidores de dominio.
Usuarios	Grupo de seguridad.	Builtin	Usuarios corrientes.

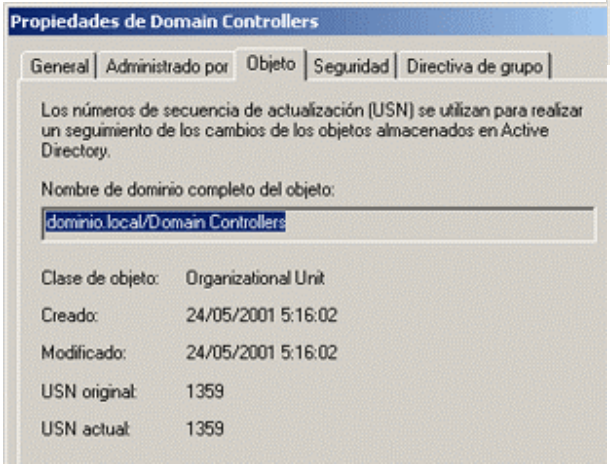
	Integración local		
Usuarios DHCP	Grupo de seguridad. Dominio local	Contenedor Users	Sus miembros sólo tienen acceso de lectura al Servidor DHCP
DnsAdmins	Grupo de seguridad. Dominio local	Contenedor Users	Administradores del DNS.
Servidores RAS e IAS	Grupo de seguridad. Dominio local	Contenedor Users	Servidores Ras e IAS.
Usuarios WINS	Grupo de seguridad. Dominio local	Contenedor Users	Sus miembros solo tienen acceso de lectura a WINS.
Publicadores de certificados	Grupo de seguridad. Global	Contenedor Users	Agentes de certificación de la empresa y de renovación.
DnsUpdateProxy	Grupo de seguridad. Global	Contenedor Users	Clientes de DNS a los que se permite realizar actualizaciones dinámicas en nombre de algunos otros clientes (como servidores DHCP).
Admins. del dominio	Grupo de seguridad. Global	Contenedor Users	Administradores designados del dominio.
Equipos del dominio	Grupo de seguridad. Global	Contenedor Users	Todas las estaciones de trabajo y servido res unidos al dominio.
Controladores de dominio	Grupo de seguridad. Global	Contenedor Users	Todos los controladores de dominio del dominio.
Invitados del dominio	Grupo de seguridad. Global	Contenedor Users	Todos los invitados del dominio.
Usuarios del dominio	Grupo de seguridad. Global	Contenedor Users	Todos los usuarios del dominio.
Administración de empresas	Grupo de seguridad. Global	Contenedor Users	Administradores designados de la empresa.
Administradores	Grupo de	Contenedor	Administradores designados del

de esquema	seguridad. Global	Users	esquema.
Administrador	Usuario	Contenedor Users	Cuenta predefinida para administrar el equipo/dominio.
Invitado	Usuario	Contenedor Users	Cuenta predefinida para el acceso en calidad de invitado al equipo/dominio.
IUSR_xxx	Usuario	Contenedor Users	Cuenta predefinida para el acceso anónimo a los Servicios de Internet información Server (IIS).
IWAM_xxx	Usuario	Contenedor Users	Cuenta predefinida para el acceso anónimo a aplicaciones IIS sin proceso.
Krbtgt	Usuario	Contenedor Users	Cuenta del servicio Centro de distribución de claves.

7.12.-Creación de unidades organizativas

El esquema del servicio de directorio establece qué objetos se pueden crear en un dominio Active Directory, dónde se pueden ubicar y qué atributos se permite que tengan. Usuarios y equipos de Active Directory solo permite crear objetos en las ubicaciones apropiadas para el tipo de objeto. Por ejemplo, no se puede crear un objeto unidad organizativa (OU) subordinada a un objeto usuario, pero un objeto usuario puede subordinarse a un objeto OU.





Sin embargo, las OU se pueden subordinar unas a otras y el número de capas de OU que se pueden crear en el dominio Active Directory es ilimitado. Para crear una OU hay que pulsar el objeto dominio u otra OU en el panel de ámbito o en el de resultados de Usuarios y equipos de Active Directory y escoger Nuevo en el menú Acción y seleccionar Unidad organizativa. también se puede pulsar el

botón Crear un nuevo departamento en la barra de herramientas de Usuarios y equipos de Active Directory para conseguir el mismo efecto. después de especificar un nombre para el nuevo objeto en el cuadro de dialogo Nuevo objeto, el administrador crea un icono con el nombre apropiado y lo inserta en la pantalla de Usuarios y equipos de Active Directory.

Una vez que se ha creado una OU es posible poblarla con otros objetos, como usuarios, equipos, grupos y otras OU, o se pueden modificar sus atributos abriendo la ventana Propiedades desde el menú Acción.

Configuración de los objetos OU

La ventana Propiedades de una OU consta de tres pestañas. La pestaña General y la pestaña Administrado por permiten especificar información sobre la OU como una frase descriptiva y una dirección para la ubicación del objeto, además de la identidad de la persona responsable de administrar la OU. La información que se incluye en estas pestañas (si la hay) depende del criterio utilizado para diseñar el Active Directory. Una OU puede estar asociada a un departamento particular dentro de una organización, una ubicación física como una habitación, una planta o un edificio, o incluso una sucursal en una ciudad o país particular.

La pestaña Directiva de grupo es donde se crean y administran los vínculos a los objetos directiva de grupo de Active Directory. Los objetos directiva de grupo son colecciones de parámetros del sistema que controlan la apariencia y la funcionalidad de los clientes de la red. Cuando se aplican directivas de grupo a OU, dominios y sitios, todos los objetos contenidos en esas entidades heredan los parámetros del sistema. Las OU se pueden enlazar a múltiples objetos directiva de grupo en esta pestaña y, se pueden controlar las prioridades con que se aplican las directivas. Cuando se utilice el botón Modificar de la pestaña directiva de grupo para modificar un objeto directiva de grupo, Usuarios y equipos de Active Directory ejecuta el complemento MMC directiva de grupo.

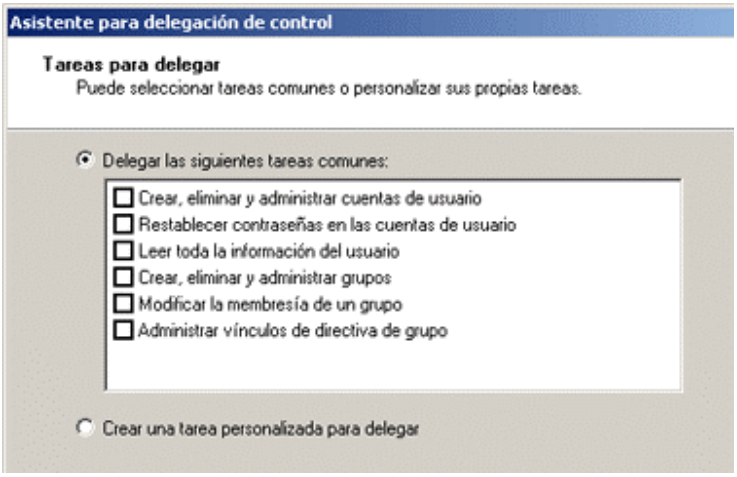
Cuando se activan las Características avanzadas en el menú Ver de Usuarios y equipos de Active Directory, la ventana Propiedades de la OU también muestra la pestaña Objeto y la pestaña Seguridad. La pestaña Objeto muestra la ruta de acceso complete al objeto en la jerarquía del dominio, las fechas y horas de su creación y ultima modificación y los números de secuencia de actualización de la creación y la ultima modificación.

La pestaña Seguridad permite controlar el acceso al objeto asignando permisos a usuarios y grupos. Con la casilla de verificación Hacer posible que los permisos heredables se propaguen, también se puede controlar si el objeto hereda los permisos que han sido asignados a su objeto primario.

El botón Avanzada de la pestaña Seguridad proporciona acceso al cuadro de dialogo Configuración de control de acceso desde el que se puede controlar el acceso al objeto con un detalle mucho mayor. En el cuadro de dialogo Seguridad, se puede especificar si usuarios y grupos específicos tienen permiso para crear y eliminar objetos secundarios en la OU, pero esta pantalla permite especificar que tipos de objetos se pueden crear y eliminar.

Delegación del control de los objetos

Active Directory esta diseñado para soportar redes empresariales mucho mas grandes que la que soportan los dominios Windows NT, y las redes mas grandes requieren, naturalmente, mas atención y mantenimiento por parte de los Administradores. Active Directory permite a los administradores delegar el control sobre objetos contenedor específicos a otros usuarios sin otorgarles acceso completo al dominio. Para hacer esto, hay que ejecutar el Asistente para delegación de control escogiendo Delegar control desde et menú Acción de un dominio o unidad organizativa.



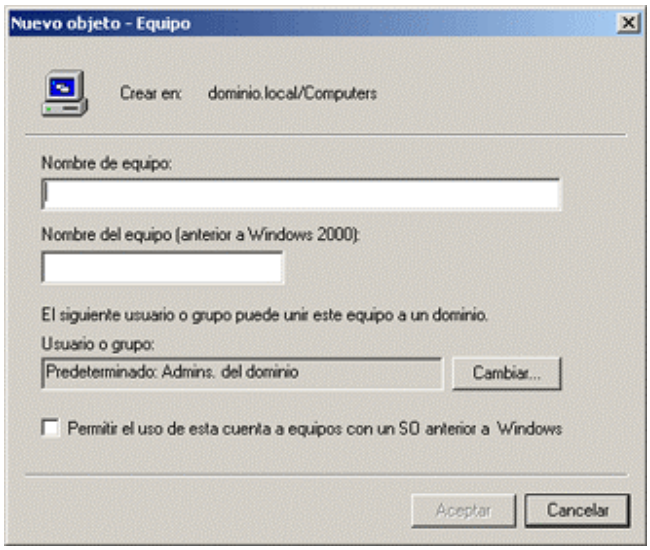
El asistente pide primero que se especifique el objeto contenedor sobre el que se desea delegar el control y los usuarios o grupos (o ambos) a los que se desea delegar el control. Una vez que se haya hecho esto, el asistente muestra la pantalla Tipo de objeto de Active Directory, que se puede utilizar para especificar que tipos de objetos del contenedor podrán controlar los usuarios/grupos seleccionados. Se puede, por ejemplo, conceder a un usuario o grupo especifico control sobre los objetos usuario solo en el contenedor, permitiéndoles actualizar información de usuario pero impidiéndoles la modificación de otros tipos de objetos.

En el cuadro de dialogo Permisos, se especifica el grado de control que se desea que tengan los usuarios/grupos seleccionados sobre los objetos seleccionados. El cuadro Mostrar estos permisos permite seleccionar si se desea trabajar con los permisos generales que conciernen a todo el objeto o los permisos de la propiedad que controlan el acceso a los atributos individuales del objeto. Con este tipo de permisos se puede conceder a los usuarios la capacidad de modificar algunas de las propiedades del objeto al mismo tiempo que se protegen otras. De esta forma, cabe la posibilidad de permitir a los Administradores del departamento realizar modificaciones sencillas en los objetos usuario, como cambiar las direcciones y los números de teléfono, sin poner en peligro otras propiedades del objeto.

Una vez que se le ha proporcionado al asistente la información apropiada, se configura el objeto seleccionado con los permisos adecuados. Si se comprueba la pestaña Seguridad de la ventana Propiedades del objeto (que solo es visible cuando están activas las Características avanzadas en el menú Ver de Usuarios y equipos de Active Directory), se podrán observar los permisos que ha asignado el asistente a los usuarios o grupos seleccionados.

7.13.-Creación de los objetos equipo

Además de objetos contenedor, objetos grupo y objetos usuario, Active Directory también tiene objetos que representan equipos. Para iniciar sesión en un dominio, un equipo Windows 2000 debe tener un objeto que lo represente en la jerarquía de Active Directory. Cuando se promueve un sistema a controlador de dominio o se inicia sesión en un dominio por primera vez, Windows 2000 crea automáticamente un objeto equipo. (En el caso de un inicio de sesión por primera vez, el sistema solicita el nombre de usuario y la contraseña de una cuenta con suficientes privilegios para crear nuevos objetos. Sin embargo, también se pueden crear objetos equipo manualmente, de igual forma que se crearía cualquier otro objeto).



Si se selecciona un contenedor, se escoge Nuevo en el menú Acción y se selecciona Equipo, se muestra un cuadro de dialogo Nuevo objeto en el que se puede suministrar el nombre del nuevo objeto equipo (que puede ser el nombre NetBIOS o el DNS del equipo). también se puede especificar el usuario o grupo particular que esta autorizado para unir el equipo al dominio.

El complemento Usuarios y equipos de Active Directory crea un objeto cada vez, pero algunas veces los administradores tienen que crear muchísimos objetos, por lo que esta herramienta deja de ser práctica.

Configuración de los objetos equipo

Una vez que Usuarios y equipos de Active Directory crea el objeto equipo, se pueden configurar sus atributos utilizando las siguientes siete propiedades: General, Sistema operativo, Miembro de, ubicación, Administrado por, Objeto y Seguridad. Casi todas las pestañas tienen el mismo propósito que las de otros objetos. Las dos que son únicas para el objeto Equipo son Sistema operativo y ubicación.

La pestaña Sistema operativo identifica el sistema operativo que se esta ejecutando en el equipo, la versión y el service pack instalado actualmente. Estos campos no son modificables; están en blanco cuando se crea manualmente un objeto equipo y se rellenan cuando el equipo se une a un dominio. La pestaña ubicación permite especificar que ubicaciones sirve el sitio en la configuración del directorio.

Administración remota de equipos

Usuarios y equipos de Active Directory proporciona acceso administrativo a equipos remotos representados por objetos en Active Directory. Cuando se pulsa un objeto equipo y se

escoge Administrar en el menú Acción, el administrador abre el complemento MMC Administración de equipos con el equipo come foco. Con esta característica, se pueden leer los registros de sucesos del sistema remote, manipular sus servicios y realizar cualquiera del resto de las tareas que proporciona el complemento administración de equipos.

7.14.-Publicación de carpetas compartidas

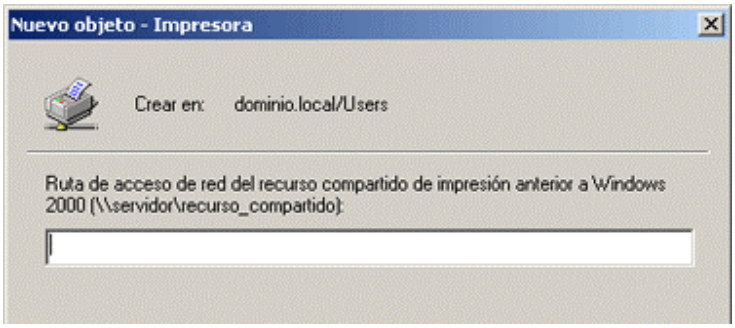
Los objetos carpeta compartida permiten publicar directorios de red compartidos en Active Directory, lo que permite a los usuarios acceder a ellos directamente explorando el Entorno de red del objeto. Esto elimina la necesidad de que los usuarios conozcan la ubicación exacta de la carpeta compartida. La creación de un objeto carpeta compartida no crea realmente el recurso compartido; hay que hacer esto manualmente en la pestaña Compartir de la ventana Propiedades de la unidad de disco o de la carpeta en la ventana del Explorador de Windows o en la ventana Mi PC. también se pueden crear objetos carpeta compartida para carpetas del Sistema de archivos distribuidos (DFS, Distributed File Sytem).

Para crear un objeto carpeta compartida, hay que pulsar un objeto contenedor en Usuarios y equipos de Active Directory, escoger Nuevo en el menú Acción y seleccionar Carpeta compartida. En el cuadro de dialogo Nuevo objeto, hay que especificar un nombre para el nuevo objeto a introducir la ruta de acceso UNC al recurso compartido. después de que el administrador cree el objeto, es posible configurarlo utilizando las pestañas de la ventana Propiedades del objeto.

Los permisos que se establecen en la pestaña Seguridad de la ventana Propiedades de la carpeta compartida no controlan el acceso a la propia carpeta compartida, solo al objeto carpeta compartida. Para acceder a la carpeta por medio de Active Directory, un usuario debe tener permiso para acceder tanto al recurso compartido como al objeto. Lo mismo es cierto para un objeto impresora.

7.15.-Publicación de impresoras

La creación de objetos impresora permite a los usuarios acceder a las impresoras a través de Active Directory prácticamente de la misma forma en que acceden a las carpetas compartidas. Un objeto impresora se crea como se haría con un objeto carpeta compartida, seleccionando un contenedor y escogiendo Nuevo\Impresora en el menú Acción y especificando la ruta de acceso UNC a la impresora compartida. El administrador crea entonces el objeto, combinando el nombre del sistema anfitrión y el del recurso compartido para formar el nombre del objeto.



7.16.-Traslado, cambio de nombre y eliminación de objetos

Una vez que se han creado objetos en Active Directory, se puede utilizar Usuarios y equipos de Active Directory para remodelar el árbol en cualquier momento trasladando objetos a diferentes contenedores, cambiándoles el nombre y eliminándolos. El menú Acción de casi cualquier objeto Active Directory contiene un comando Mover, que abre un cuadro de dialogo en el que se puede buscar un contenedor donde situar el objeto. También se pueden seleccionar varios objetos manteniendo presionada la tecla CTRL mientras se pulsa en ellos con el ratón y moviéndolos al mismo contenedor.

Cuando se traslada un objeto contenedor a una nueva ubicación, se trasladan automáticamente todos los objetos incluidos en el contenedor al mismo tiempo y también se modifican las referencias a esos objetos en el resto de objetos de Active Directory. Si, por ejemplo, el Usuario X es un miembro del Grupo Y y se traslada la unidad organizativa que contiene el objeto usuario de X a una nueva ubicación, X sigue siendo miembro de Y, y la lista de miembros del Grupo Y se actualiza automáticamente para mostrar a X en su nueva ubicación. De la misma forma, cuando se cambia el nombre de un objeto utilizando el comando Cambiar nombre del menú Acción o pulsando sobre el objeto una vez, todas las referencias a ese objeto a lo largo de Active Directory Cambian para reflejar el nuevo nombre. Cuando se elimina un objeto contenedor, todos los objetos incluidos en el contenedor se eliminan también.

La tarea central de una red es asegurar que los clientes (los usuarios) tengan todo lo que necesitan y nada que no necesitan. Lo que necesitan incluye acceso a los archivos, carpetas, aplicaciones, impresoras y conexiones de Internet que requieren para hacer su trabajo. Lo que no necesitan es problemas para acceder a lo que si necesitan.

El administrador de la red tiene necesidades adicionales, como material que requiere conocimientos para protegerse de aquellos que no tienen por que tener conocimientos y proteger a los usuarios de ellos mismos. La clave de todas estas necesidades es la configuración de grupos, usuarios y directivas de grupo.

7.17.- Derechos de usuario

Derechos son aquellas acciones que los usuarios pueden o no realizar. Los derechos se aplican generalmente al sistema entero. La capacidad de hacer copia de seguridad de archivos o de iniciar sesión en un servidor, por ejemplo, es un derecho que el administrador concede o retira. Los derechos se pueden asignar de forma individual, pero la mayoría de las veces son característicos de los grupos, y un usuario se asigna a un grupo particular en base a los derechos que necesita.

Los permisos indican el acceso que un usuario (o un grupo) tiene a objetos específicos como archivos, directorios a impresoras.

Los derechos, a su vez, están divididos en dos tipos: privilegios y derechos de inicio de sesión. Los privilegios incluyen cosas como la capacidad de ejecutar auditorias de seguridad o

forzar el apagado desde un sistema remoto; obviamente cosas que no hacen la mayoría de los usuarios. Los derechos de inicio de sesión implican la capacidad de conectarse a un equipo de forma especifica. Los derechos se asignan automáticamente a usuarios individuales además de a grupos. Es preferible la asignación a grupos, por lo que, en la medida de lo posible, se deberían asignar los derechos por pertenencia a un grupo para simplificar la administración. Cuando la pertenencia de los grupos define derechos, se pueden eliminar los derechos de un usuario eliminando simplemente al usuario del grupo.

Derechos de inicio de sesión asignados de forma predeterminada a los grupos		
Nombre	**Descripción**	**Grupos con el derecho asignado de forma predeterminada**
Iniciar sesión como servicio	Permite iniciar sesión como un servicio utilizando una cuenta de usuario y un contexto de seguridad específicos.	Ninguno
Iniciar sesión como trabajo de procesamiento por lotes	Permite iniciar sesión utilizando una cola de procesamiento por lotes.	Administradores
Iniciar sesión local	Permite iniciar sesión desde el teclado del equipo.	Administradores, Operadores de copia; Operadores de cuentas, Operadores de impresión, Operadores de servidores
Tener acceso a este equipo desde la red	Permite la conexión al equipo a través de la red.	Administradores, Todos, Usuarios avanzados.

Privilegios asignados de forma predeterminada a los grupos		
Privilegio	**Descripción**	**Grupos con el privilegio asignado de forma predeterminada**
Actuar como	Permite a un proceso autenticarse como	Ninguno

parte del sistema operativo	cualquier usuario. Un proceso que requiere este privilegio debería utilizar la cuenta LocalSystem, que ya incluye este privilegio.	
Administrar registros de auditoria y de seguridad	Permite a un usuario especificar opciones de auditoria y ver y borrar el registro de seguridad del Visor de sucesos. Se debe activar Auditar el acceso del servicio de directorio para que se pueda realizar la auditoria de acceso a objetos. Los administradores siempre pueden ver y borrar el registro de seguridad.	Administradores
Agregar estaciones de trabajo a un dominio	Permite a un usuario añadir nuevas estaciones de trabajo a un dominio existente.	Administradores
Apagar el sistema	Apaga Windows 2000.	Administradores, Operadores de copia, Todos, Usuarios, Usuarios avanzados
Aumentar la prioridad de programación	Permite el uso del Administrador de tareas de programación para cambiar la prioridad de un proceso.	Administradores, Usuarios avanzados
Aumentar las cuotas	Permite a un proceso con permiso de escritura acceder a otro proceso para aumentar la cuota de procesador asignada a ese proceso.	Ninguno
Bloquear paginas en la memoria	Permite a un proceso mantener información en la memoria física. Este es un privilegio obsoleto que puede tener un serio efecto negativo en el rendimiento del sistema. No se debe utilizar.	Ninguno
Cambiar la hora del sistema	Permite establecer la hora del reloj interno del equipo.	Administradores, Usuarios avanzados.
Cargar y descargar controladores de dispositivo	Instalar y desinstalar controladores de dispositivo.	Administradores
Crear objetos	Permite a un proceso crear un objeto de	Ninguno

compartidos permanentes	directorio. Lo utilizan componentes de modo de núcleo para ampliar el espacio de nombres de objetos de Windows 2000. Los componentes que se ejecutan en modo de núcleo ya tienen este privilegio.	
Crear un archivo de paginación	Permite la creación y modificación de un archivo de paginación	Administradores
Crear un objeto identificador (token)	Permite a un proceso crear un identificador (token) que se puede utilizar para acceder a cualquier recurso local. Un proceso que requiere este privilegio debería utilizar la cuenta LocalSystem, que ya incluye este privilegio.	Ninguno
Depurar programas	Permite al usuario asignar un depurador a un proceso.	Administradores
Desacoplar un equipo portátil	Permite desacoplar un portátil de una estación de acoplamiento utilizando la interfaz de Windows 2000.	Administradores, Usuarios
Forzar el apagado desde un sistema remoto	Permite apagar un equipo desde una ubicación remota de la red.	Administradores
Generar auditorias de seguridad	Permite a un proceso crear entradas en el registro de seguridad.	Ninguno
Habilitar la opción de confianza para la delegación en las cuentas de usuario y de equipo	Permite a un usuario establecer la configuración Confianza para la delegación en un objeto.	Administradores
Modificar valores del entorno del firmware	Permite la configuración de la RAM no volátil en equipos que soportan tal función.	Administradores
Omitir la comprobación	Permite a un usuario recorrer los árboles del directorio (estructuras de carpetas) incluso si	Todos

de recorrido	el usuario no tiene permiso para acceder a los directorios por los que pasa.	
Perfilar el rendimiento del sistema	Permite observar el rendimiento del sistema.	Administradores
Perfilar un único proceso	Permite observar el rendimiento de un proceso.	Administradores, Usuarios avanzados
Realizar copias de seguridad de archivos y directorios	Permite hacer copias de seguridad del sistema, ignorando los permisos específicos de archivos y carpetas.	Administradores, Operadores de copia
Reemplazar un identificador (Token) de nivel de proceso	Permite reemplazar el identificador (Token) predeterminado asociado con un subproceso.	Ninguno
Restaurar archivos y directorios	Permite restaurar archivos y carpetas en un sistema; invalida los permisos específicos de archivos y carpetas.	Administradores, Operadores de copia
Sincronizar información del servicio de directorio	Permite a un usuario iniciar una sincronización del Active Directory.	Administradores
Tomar posesión de archivos y otros objetos	Permite a un usuario tomar posesión de cualquier objeto de seguridad incluyendo archivos y carpetas, impresoras, claves de registro y procesos. Invalida los permisos específicos.	Administradores