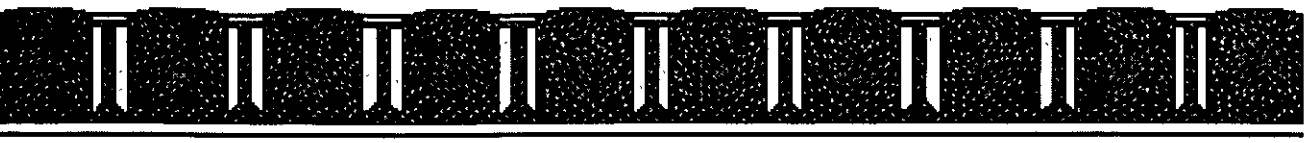


FACULTAD DE INGENIERÍA UNAM
DIVISIÓN DE EDUCACIÓN CONTINUA

MATERIAL DIDACTICO DEL CURSO

WINDOWS 2003 SERVER

10 al 14 de octubre de 2007

Palacio de Minería, Calle de Tacuba # 5-Entrepiso, Centro Histórico, Delegación Cuauhtémoc, Código Postal 06000,
México D.F. Tel/FAX 5510-4673, Teléfonos 5623-2947 y 5623-2960

Facultad de Ingeniería

Unidad de Servicios de Cómputo Académico

WINDOWS 2003 SERVER®

WINDOWS 2003 SERVER®

Realizó:

Flores Alvarez Luis Armando

Guerrero Martínez Edson Armando

Octubre 2007

WINDOWS 2003 SERVER®

Tema 1

Protocolo TCP/IP

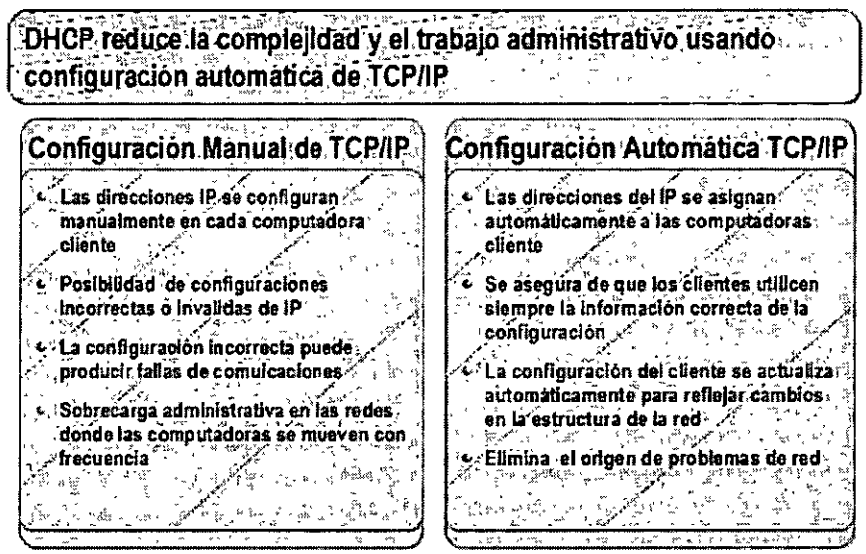
- Asignación y administración de direcciones fijas y dinámicas (DHCP)
- Asignación de nombre y dirección de equipos (DNS)
- Iniciar sesión de Windows Server 2003 ®
- Manejo de paquetería usando Network Monitor

FLORES ALVARES LUIS ARMANDO
GUERRERO MARTINEZ EDSON ARMANDO

Asignación y administración de direcciones fijas y dinámicas (DHCP)

DHCP (Dynamic Host Configuration Protocol) es un protocolo desarrollado para asignar direcciones IP a los clientes que las soliciten facilitando la administración. El estándar DHCP permite que usted utilice los servidores de DHCP para manejar la asignación dinámica de las direcciones y la configuración de otros parámetros IP para clientes DHCP en su red.

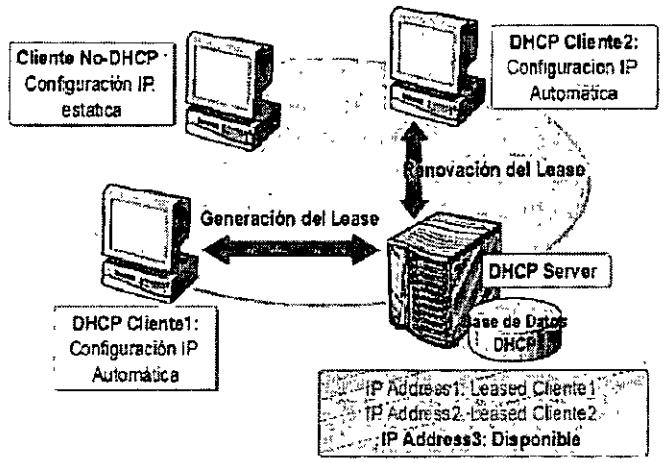
En redes TCP/IP, DHCP reduce la complejidad y el trabajo administrativo de re-configurar las computadoras cliente. Permite manejar la asignación de IP de una localización central, y por lo tanto se puede configurar el DHCP Server para asignar a una sola subnet o múltiples subnets.



¿Qué son los DHCP Scopes?

Un *scope* es un rango de direcciones válidas IP que están disponibles para asignar las computadoras cliente en una subnet en particular. Un scope tiene las siguientes características:
Network ID: El Network ID para el rango de direcciones IP.
Subnet mask: La subnet mask para el Network ID.
Network IP address range: El rango de direcciones IP disponibles para los clientes.
Lease duration: El período de tiempo que el DHCP Server asigna a la dirección del cliente.
Router: La dirección del Default Gayeway.
Scope name: Identificador para propósitos administrativos.
Exclusion range: El rango de direcciones IP en el scope excluidas para la asignación.

El lease es el espacio de tiempo en el cual un cliente DHCP puede utilizar una configuración dinámicamente asignada de IP. Antes de la expiración del tiempo lease, el cliente debe renovarlo u obtener uno nuevo del DHCP.



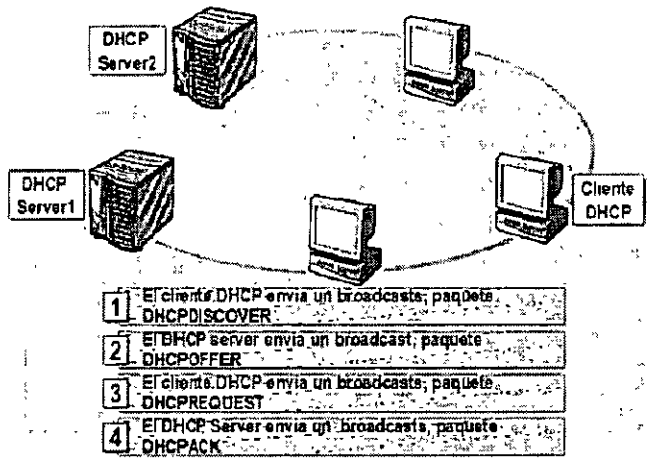
Proporciona las siguientes ventajas:

Una configuración segura y fiable, ya que evita los errores de configuración producidos al escribir manualmente valores en cada equipo. Así mismo, ayuda a evitar los conflictos de direcciones causados al asignar direcciones IP que ya están siendo utilizadas en la red.

Reduce la administración de la configuración. La utilización de servidores DHCP puede reducir significativamente el tiempo necesario para configurar y reconfigurar los equipos de la red.

El proceso a seguir por un cliente DHCP es el siguiente:

1. Manda un mensaje al servidor DHCP solicitando una dirección IP.
2. El servidor DHCP responde ofreciendo las direcciones IP que tiene disponibles.
3. El cliente selecciona y envía una solicitud de uso de la dirección al servidor DHCP.
4. El servidor DHCP admite la solicitud y garantiza al cliente la concesión del uso de la dirección durante el tiempo determinado.
5. El cliente utiliza la dirección para conectarse a la red.



¿Cómo funciona el proceso DHCP Lease Renewal?
DHCP Lease Renewal Process es el proceso por el cual un cliente DHCP renueva o actualiza sus datos de configuración IP con el DHCP Server. El cliente DHCP renueva la configuración IP antes de la expiración del tiempo de lease. Si el período de lease expira y el cliente DHCP todavía no ha renovado su configuración IP, pierde los datos de la configuración IP y comienza nuevamente el proceso DHCP Lease Generation.

La autorización de DHCP es el proceso de registrar el servicio DHCP Server en un dominio Active Directory Service, con el propósito de dar soporte a clientes DHCP. La autorización DHCP es solo para DHCP Servers corriendo Windows Server 2003 ® y Windows 2000 ® en Active Directory.

Como instalar un servidor DHCP

Para instalar un servidor DHCP siga los pasos siguientes:

1. Marque en el icono **Add and Remove Programs** del **Control Panel** en el menú **Start.**
2. Pulse en **Add and Remove Windows/Components.**
3. Hacer click en **Details** de **Networking Components.**
4. Activar la casilla de **Dynamic Host Configuration Protocol (DHCP)** y marque en **OK.**
5. Marque en **Next** y comenzará a configurar los componentes.
6. Cuando haya acabado, marque en Finalizar.
7. Cierre la pantalla de **Add en Remove Programs**.

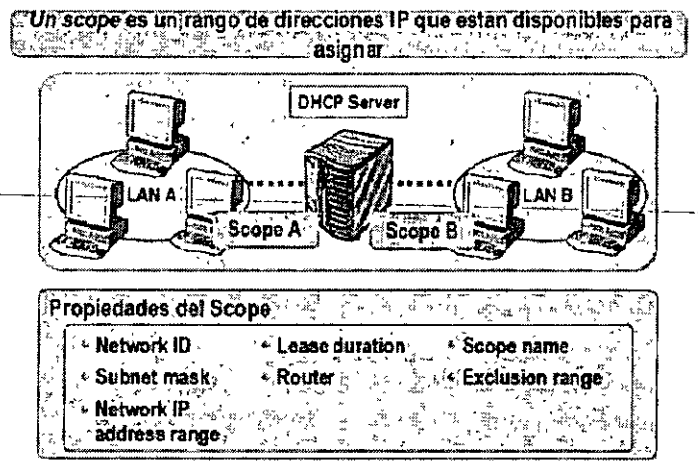
La autorización de DHCP es el proceso de registrar el servicio DHCP Server en un dominio Active Directory, con el propósito de dar soporte a clientes DHCP. Autorizar al DHCP Server provee la capacidad de controlar la adición de los DHCP Servers al dominio. La autorización debe ocurrir antes de que el DHCP pueda otorgar leases a clientes DHCP.

Solicitar la autorización previene que DHCP Servers desautorizados ofrezcan direcciones IP inválidas a clientes.

Como autorizar el servicio DHCP Server

1. Abrir la consola **DHCP**.
2. Seleccionar el Server en la consola.
3. Hacer clic en **Authorize** del menú **Action.**
4. Para verificar que el **DHCP Server** este autorizado: en la consola, presionar F5 para refrescar la vista, y verificar que el **DHCP Server** ahora se visualice con una flecha verde hacia arriba.

Un **scope** es un rango de direcciones IP validas que están disponibles para asignar las computadoras cliente en una subred en particular. Usted puede configurar un **scope** en el **DHCP Server** para determinar el pool de direcciones IP que ese Server asignara a cliente. Los **scopes** determinan las direcciones IP que se asignan a los clientes. Puede configurar tantos **scopes** en el **DHCP Server** como lo necesite para su ambiente de red.



1. Seleccione **DHCP** de **Administrative Tools** del menú **Start** , abrir la consola.

2. Hacer clic en el **DHCP Server** de la consola, dar clic derecho y seleccionar **New Scope.**

3. En el **Wizard** de **New Scope** hacer clic en **Next** y le mostrará una pantalla para que le indique el nombre que desea darle al **Scope** además de una breve descripción.

4. Configurar, en la ventana **IP Address Range**, la dirección IP inicial 192.168.1.1, la dirección IP final 192.168.1.254 y la subred mask 255.255.255.0.

5. Configurar, en la ventana **Add Exclusions**, la dirección IP inicial 192.168.1.20 y la dirección IP final 192.168.1.30, si es aplicable.

6. Configurar, en la página **Lease Duration**, los días, horas y minutos. (El default es 8 días)

7. Configurar **DHCP Options** y seleccionar **Yes, I want to configure these options now** para configurar las opciones del DHCP Server ahora.

8. En la ventana **Router (Default Gateway)** indique la IP del router o gateway y pulse en **Add**. Si se dispone de más de uno indíquelos, sino de clic en **Next.**

9. En la ventana **Domain Name and DNS Servers**, indicar el dominio principal **DNS**, también podemos poner el nombre del servidor y pulsar en **resolve** y automáticamente escribirá su dirección IP, en caso de no conocerla. Podemos también en caso de no conocer el nombre del servidor **DNS**, poner la IP y pulsar en **Add** en ambos casos para que pase al apartado correspondiente. Marque en **Next** si ha terminado.

10. En la siguiente pantalla aparecerá la configuración de un servidor **WINS** si se tiene instalado uno. En caso afirmativo, al igual que cuando configuramos el **DNS Server**, podemos conocer la IP y agregarla con **Add** o podemos conocer sólo el nombre y pulsar **Resolve** y nos dará la IP que deberemos agregar al apartado correspondiente. Cuando haya finalizado, pulse **Next**.

11. La siguiente ventana nos preguntara si deseamos activar un ámbito **Activate scope**, para activarlo en ese momento marque en **Yes, I want to activate this scope now**, y marque en **Next**, en caso contrario esta opción estará disponible en el momento que lo requiera en el menú contextual del **DHCP Server**.

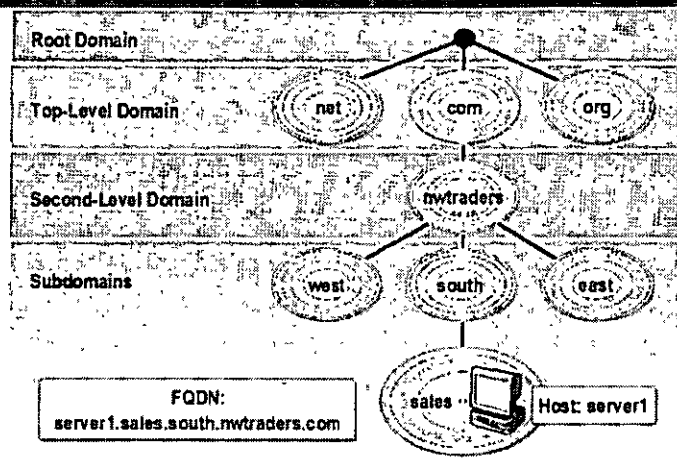
12. Pulse en la siguiente pantalla en **Finish** y volverá a la pantalla principal de la utilidad.

Asignación de nombre y dirección de equipos (DNS)

El Domain Name System (DNS) es un servicio estándar de Internet y de TCP/IP. El servicio de DNS permite a las computadoras cliente, colocar en su red y resolver nombres de dominio DNS. Una computadora configurada para proporcionar servicios del DNS en una red, es un servidor DNS, lo que es necesario para poner en funcionamiento Active Directory. La función principal es la traducción de nombres a direcciones IP y viceversa.

¿Qué es el Domain Namespace?

El Domain Namespace es un árbol de nombres jerárquico que utiliza DNS para identificar y localizar un host en un dominio dado, concerniente a la raíz del árbol. Los nombres en la base de datos DNS establecen una estructura lógica llamada Domain Namespace, que identifica la posición de un dominio en el árbol y su dominio superior. La convención principal es simplemente ésta: para cada nivel de dominio, un punto (.) se utiliza para separar a cada descendiente del subdominio y de su dominio de nivel superior.



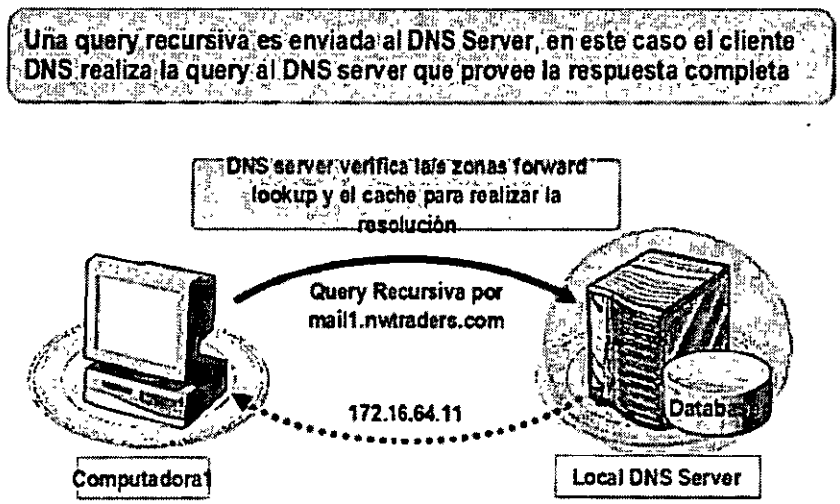
¿Cómo se almacenan y se mantienen los datos DNS?

Una zona es una parte contigua del espacio de nombres de dominio en el que un servidor DNS tiene autoridad para resolver consultas DNS. El espacio de nombres DNS se puede dividir en diferentes zonas, que almacenan información de nombres acerca de uno o varios dominios DNS, o partes de ellos. Para cada nombre de dominio DNS incluido en una zona, ésta se convierte en el origen autorizado de la información acerca de ese dominio.

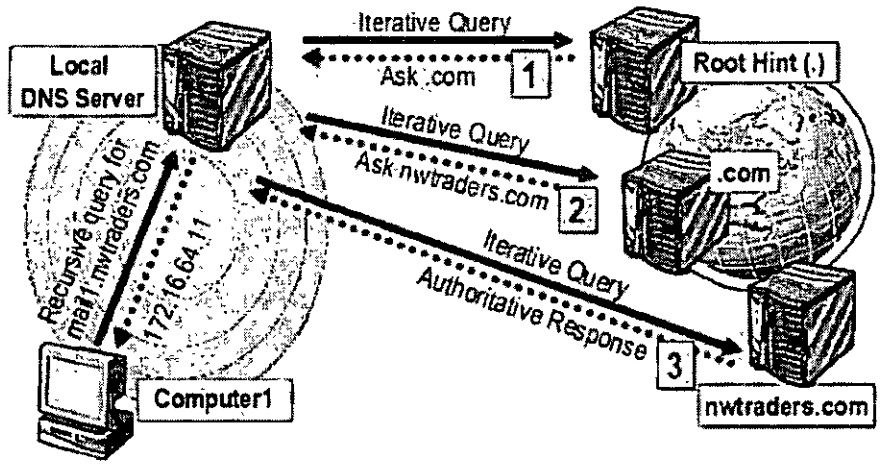
¿Qué es una Query DNS?

Una Query es una solicitud de resolución de nombre enviado a un DNS Server. Hay dos tipos de Query: Recursiva e Iterativa.

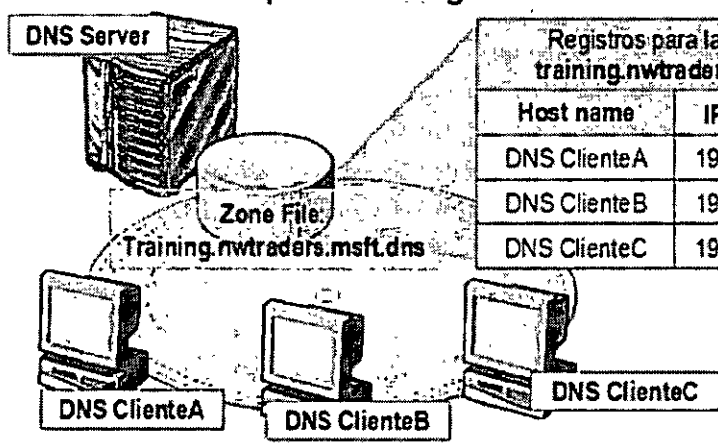
¿Cómo funciona una Query Recursiva?



¿Cómo funciona una Query Iterativa?

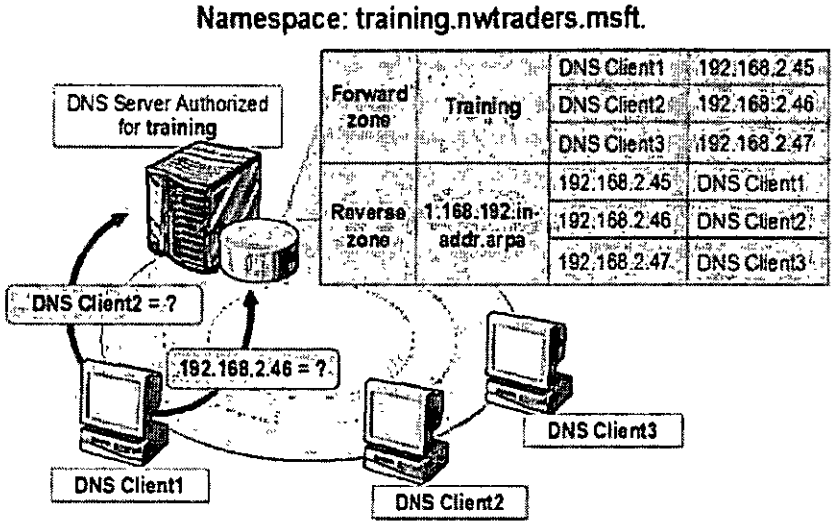


Namespace: training.nwtraders.msft

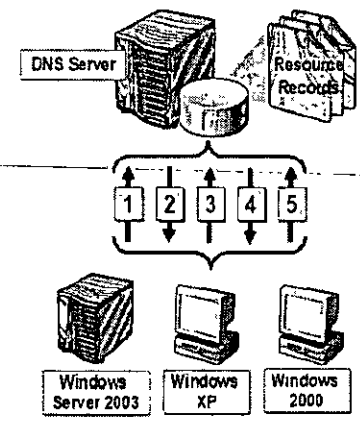


Registros para la zona training.nwtraders.msft	
Host name	IP address
DNS ClienteA	192.168.2.45
DNS ClienteB	192.168.2.46
DNS ClienteC	192.168.2.47

Creación de zonas de búsqueda estándar



Introducción a las actualizaciones dinámicas



El protocolo de actualización dinámica permite a los equipos cliente actualizar automáticamente sus registros de recursos en un servidor DNS sin necesidad de intervenir el administrador. De forma predeterminada, los equipos con Windows 2000 ®, Windows XP ® y Windows Server 2003 ® se configuran para realizar actualizaciones dinámicas cuando también se configuran con una dirección IP estática.

I. Instalar el Servicio de Servidor DNS

Antes de instalar **Active Directory** es necesario tener implementado una infraestructura de DNS para soportar el **Active Directory**

1. Configurar el sufijo de DNS en la computadora. El sufijo DNS debe ser el asignado a cada participante: ***dominio.unam.mx***

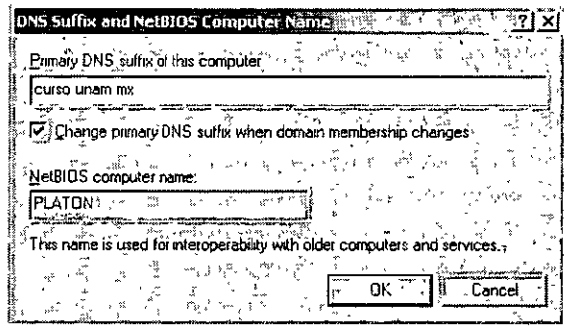
a) Iniciar sesión como administrador

b) Abrir el cuadro de **Properties** de **My Computer**

c) En la pestaña de **Computer Name** del cuadro de dialogo de **System Properties** dar clic **Properties**

d) En el botón de **change** dar clic en **More**

e) En el cuadro de dialogo **Primary DNS suffix of this Computer**, se debe escribir el nombre de dominio asignado, ***dominio.unam.mx*** además de activar la casilla de **Primary DNS suffix when domain membership changes on this computer**, después dar **ok**



f) Dar clic en **OK** para cerrar el cuadro de dialogo **Identification Changes**, y después dar clic en **OK** para cerrar el cuadro de dialogo

g) Dar clic en **OK** para cerrar el cuadro de **Properties** y después se requiere reiniciar el sistema para que hagan efecto los cambios.

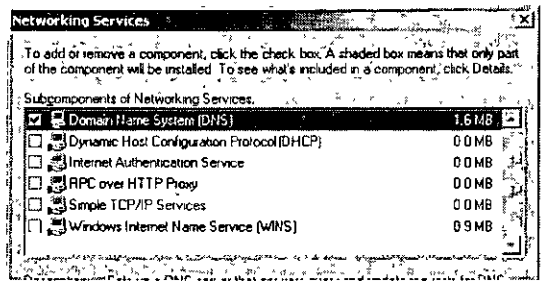
2. Iniciar el **Windows Components Wizard** e instalar el subcomponente de **Domain Name System (DNS)** de **Newtworking Services**. Copiar los archivos requeridos del CD de Windows 2003 Server ®.

a) Iniciar sesión con la cuenta de Administrador

b) En el panel de control dar doble clic en **Add/Remove Programs** y después dar clic en **Add/Remove Components**

c) En la página de **Windows Components**, bajo **Components**, dar clic en **Nerworking Services** y después dar clic en **Details**

d) Bajo **Networking Services** se debe sólo verificar que todos los cuadros de verificación NO estén seleccionados y seleccionar sólo el cuadro de verificación **Domain Name System (DNS)** y después dar clic en **OK.**



e) En el **Windows Components Wizard** dar clic en **Next.**

f) Si se requiere, inserte el cd de Windows 2003 Server ® y después de clic en **OK.**

g) Después de que los archivos requeridos hayan sido copiados, dar clic en **Finish**, y después cerrar todas las ventanas.

II. Crear Zonas Directas e Inversas

Después de instalar el DNS, se debe de configurar una zona de búsqueda directa para resolver los nombres de servidor a direcciones IP y una zona de búsqueda inversa para resolver las direcciones IP a nombre de servidor.

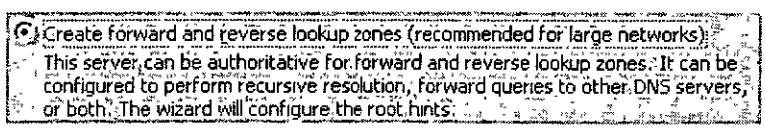
1. Agregar zonas de búsqueda directa e inversa estándar para ***dominio.unam.mx*** y el Network ID apropiado

a) Dar clic en **Start,** seleccionar **Programs**, **Administrative Tools** y después dar clic en **DNS**

b) En el árbol de consola, dar clic derecho sobre computadora (nombre de computadora actual) y después dar clic en **Configure the Server**

c) En la página **Welcome to the Configure DNS Server Wizard** dar clic en next

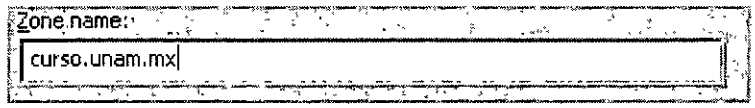
d) En la página **Select configuration action** seleccionar la opción **Create a forward and reverse lookup zones** y después dar clic en **Next**



e) En la página de **Forward Lookup Zone** seleccionar la opción **Yes, create a forward lookup zone now**

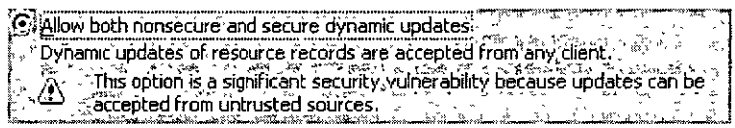
f) En la página **Zone Type** se debe de verificar que sea **Primary Zone** y dar clic en **Next**

g) En la página **Zone Name**, en el cuadro **Name** escriba ***dominio.unam.mx*** (dominio es el nombre asignado) y después dar clic en **Next**



h) En la página **Zone File**, se debe verificar que **Create a new file with this file name** este seleccionado y después dar clic en **Next**

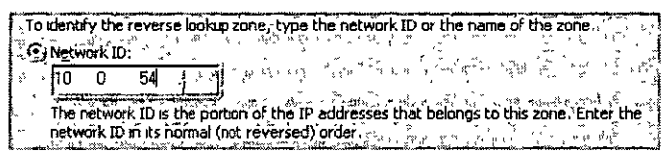
i) En la página **Dynamic Update** seleccionar **Allow both none secure and secure dynamic updates**, dar clic en **Next**



j) En la página de **Reverse Lookup Zone** seleccionar la opción **Yes, create a reverse lookup zone now**, dar clic en **Next**

k) En la página **Zone Type** se debe de verificar que sea **Primary Zone** y dar clic en **Next**

l) En la página **Zone Name**, verificar que **Network ID** este seleccionado. Para el **Network ID**, escriba los primeros tres octetos de las direcciones IP de la computadora y después dar clic en **Next**



m) En la página **Zone File**, se debe verificar que **Create a new file with this file name** este seleccionado y después dar clic en **Next**

n) En la **página Dynamic Update** seleccionar **Allow both none secure and secure dynamic updates**, dar clic en **Next**

o) En la página de **Forwardes** , selecciona **No, it should not forward queries,** clic en **Next**

p) En la página de **Completing the Configure DNS Server Wizard** dar clic en **Finish**

2. Configurar las propiedades del Protocolo TCP/IP en las conexiones de área local para utilizar a la computadora como DNS

a) Ir a las **Properties** de **TCP/IP** y en **Use the following DNS Server addresses** escribir la IP asignada a la computadora y dar **OK**

3. Utilizar el comando ipconfig para registrar los registros DNS de la computadora.

a) Abra una ventana de línea de comandos

b) En la línea de comandos, escriba ipconfig /registerdns y presionar enter

c) Cerrar la línea de comandos

4. Actualizar el **DNS** para mostrar el registro de recurso de apuntador en la zona de búsqueda inversa.

a) Abrir la consola **DNS**

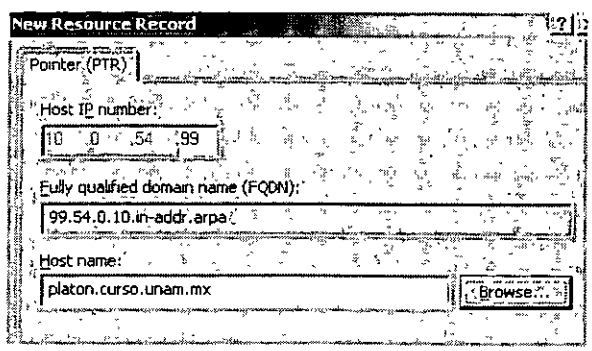
b) En el menú **Action** dar clic en **Refresh** . Aparecerá un nuevo registro de recurso de apuntador en la zona de búsqueda inversa **10.0.54.x** . Si no apareciera abrá que hacerlo manual mente, sino cerrar la ventana **DNS**

Crear el Apuntador en la zona de búsqueda Inversa

a) Expandir **Reverse Lookup Zones** en la consola **DNS**

b) Dar clic derecho sobre **10.0.54.x subnet** para el ejemplo y dar **new Pointer (PTR)**

c) En la ventana de **New Resource Record** indicar la ip que se asigno en el campo de **Host IP number**



d) En **Host name** seleccionar el **Host** al cual se va a ligar el apuntador y después dar **OK**

e) En el menú **Action** dar clic en **Refresh,** cerrar la ventana **DNS**

II. Utilizar Nslookup para probar el DNS

1. Confirmar que el **DNS** puede resolver un nombre de servidor a una dirección IP

a) Abra una ventana de línea de comandos
b) En la línea de comandos escriba ***nslookup computadora.dominio.unam.mx*** y presionar enter

2. Confirmar que el **DNS** pueda resolver una dirección IP a un nombre de servidor

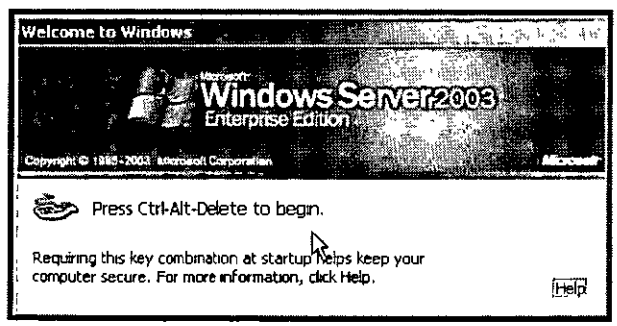
a) En la línea de comandos escriba ***nslookup direccion IP*** y después presionar Enter

b) Cerrar las ventanas

Iniciar sesión en Windows Server 2003 ®

La **Autenticación** verifica la identidad de algo o alguien. La identidad de un usuario o equipo debe ser autenticada antes de que tengan acceso a archivos, carpetas, impresoras y aplicaciones. Este proceso consta de dos partes fundamentales: las *credenciales* y la *validación*.

En Windows Server 2003 ® la combinación de las teclas Ctrl+Alt+Supr, es decir pulsar al mismo tiempo las teclas Control+Alt+Suprimir, muestra la ventana de inicio de sesión.



Tipos de inicio de sesión

- Inicio de sesión Local (**Local logon**)

Este inicio es comprobado por la base de datos SAM (**S**ecurity **A**ccounts **M**anager) en el equipo físico donde se procede a iniciar la sesión, así como se tendrá acceso sólo a los recursos del mismo equipo físico.

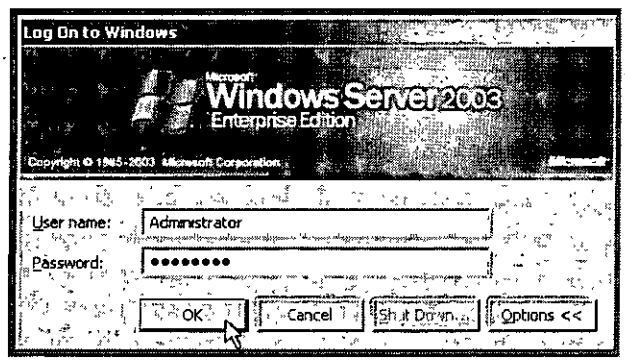
- Inicio de sesión Dominio (**Domain Logon**):

Este inicio es comprobado por un Controlador de Dominio (DC). Se tiene acceso a los recursos en el dominio y en cualesquiera dominios de confianza.
- Se inicia sesión en el dominio, las credenciales del usuario son cifradas y enviadas a un DC, éste determina a qué grupos pertenece el usuario y devuelve un token de acceso y el usuario accede a la red.

- Inicio de sesión secundario (**Secondary Logon**)

Mediante este inicio los administradores pueden iniciar sesión con una cuenta que no es de administrador y ejecutar aplicaciones en un contexto de administrador. Cuando se usa este inicio para abrir un programa, herramienta u otro, se tiene los derechos y privilegios del usuario con que se inicia para ese programa, herramienta u otro sólo.
Este inicio se comprueba por un Controlador de Dominio y se tiene acceso a los recursos del dominio y de aquéllos con que se mantiene relaciones de confianza.

Este cuadro de diálogo nos muestra lo siguiente:



Nombre de usuario (User name) : Un nombre único asignado por un administrador a la cuenta del usuario.

Contraseña (Password): La contraseña que ha sido asignada a la cuenta del usuario. Normalmente el propio usuario puede definirla, la contraseña es case sensitive, quiere decir que diferencia entre mayúsculas y minúsculas. Aparece en la pantalla como asteriscos * en el momento que se introduce. Y normalmente debería cumplir ciertas condiciones para ser una contraseña fuerte y segura.

Inicio en (Log on To): Esto no aparece si el equipo no pertenece a un dominio. Aquí aparece una lista de posibilidades: El nombre del dominio al que pertenece el equipo y el nombre del equipo por si se desea iniciar sesión localmente (Si el equipo es un DC ésta

opción nunca aparecerá); también aparecerán aquéllos dominios que pertenezcan al árbol de dominios.

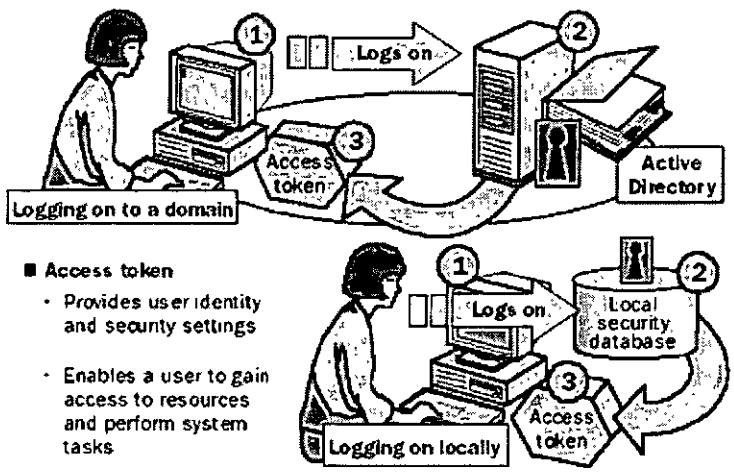
Luego los botones de Ok, Cancelar, Shutdown y Opciones.

Shutdown puede aparecer difuminado, por lo que no está activado, y el de opciones efectúa el simple cambio de mostrar el apartado de Inicio en (Log on To) o no mostrarlo.

Proceso de Autenticación de Windows 2003 Server ®

Para acceder a un equipo con Windows 2003 Server ® o a cualquier recurso en ese equipo, un usuario debe proporcionar un nombre de usuario y una contraseña. La forma que tiene Windows 2003 Server ® de autenticar un usuario varía en función de que el usuario haya realizado un inicio de sesión en un dominio o localmente en un equipo. La autenticación verifica la identidad de algo o alguien. La identidad de un usuario o un equipo debe ser autenticada antes de que estos tengan acceso a los archivos, directorios y aplicaciones. Debemos decir que la autenticación tiene dos partes fundamentales:

- Credenciales: como la combinación una cuenta y una contraseña, sostiene la identidad del usuario.
- Validación: confirma o deniega la validación de las credenciales, determinando el nivel de confianza concedida al usuario.



Los pasos en el proceso de autenticación son los siguientes:

1. El usuario inicia la sesión proporcionando información de inicio de sesión que incluye el hombre de usuario y la contraseña.

- Si el usuario inicia la sesión en un dominio, Windows 2003 Server ® redirige esta información cifrada a un controlador de dominio.

- Si el usuario inicia la sesión localmente, Windows 2003 Server ® redirige esta información al subsistema de seguridad del equipo local.

2. Windows 2003 Server ® compara la información de inicio de sesión con la información sobre el usuario que esté almacenada en la base de datos correspondiente.

- Si el usuario ha iniciado la sesión en un dominio, el controlador de dominio contiene una copia del directorio que Windows 2003 Server ® utiliza para validar la información de inicio de sesión.

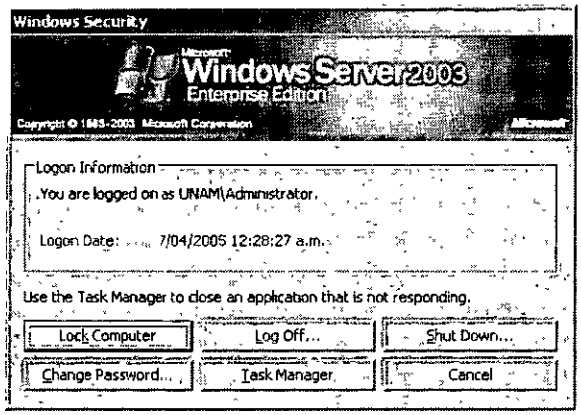
- Si el usuario ha iniciado la sesión de manera local, el subsistema de seguridad del equipo local contiene la base de datos local de seguridad que Windows 2003 Server ® utiliza para validar la información de inicio de sesión.

3. Si la información coincide y la cuenta de usuario se habilita, Windows 2003 Server ® crea un token de acceso para el usuario. Un token de acceso es la identificación del usuario para los equipos del dominio o para el equipo local, y contiene las configuraciones de seguridad, que incluye el identificador de seguridad de usuario (SID - Security ID). Estas configuraciones de seguridad permiten al usuario acceder a los recursos apropiados y poder realizar tareas específicas del sistema. El SID es un número único que identifica al usuario, al grupo y a las cuentas del equipo.

4. Si la información de inicio de sesión no coincide o la cuenta de usuario no se valida, el acceso al dominio o al equipo local se deniega.

El Cuadro de Diálogo de Seguridad de Windows 2003 Server ®

El cuadro de diálogo Seguridad de Windows proporciona un acceso sencillo a funciones importantes de seguridad. El cuadro de diálogo Seguridad de Windows muestra la cuenta de usuario que inició la sesión, el dominio o equipo con el que el usuario ha iniciado la sesión y la fecha y hora a la que se produjo este inicio de sesión. Esta información es importante para los usuarios con varias cuentas de usuario, como es el caso de los usuarios individuales que tienen su cuenta además de otra cuenta de usuario con privilegios administrativos. Para acceder al cuadro de diálogo Seguridad de Windows, presione Ctrl+Alt+Supr (Ctrl+Alt+Del).



Los botones del cuadro de diálogo Seguridad de Windows, son:

- ***Bloquear equipo (Lock Computer)***: Permite asegurar el equipo sin tener que cerrar la sesión. Todos los programas permanecen en funcionamiento. Se debería bloquear el equipo si se deja durante un corto período de tiempo. El usuario que bloquea el equipo puede desbloquearlo presionando Ctrl+Alt+Supr a introduciendo la contraseña válida. Un administrador puede también desbloquear un equipo cerrando la sesión del usuario actual; sin embargo, este es un cierre de sesión forzado y los datos se pueden perder.

- ***Cerrar la sesión (Log off)***: Permite cerrar la sesión del usuario actual y cerrar todos los programas que se encuentran en ejecución, aunque Windows 2000 ® permanece en ejecución.

- ***Apagar (Shut Down)***: Permite cerrar todos los archivos, guardar todos los datos del sistema operativo y preparar el equipo para que se pueda apagar de una manera segura.

- ***Cambiar contraseña (Change Password)***: Permite cambiar la contraseña de la cuenta de usuario. Se debe conocer la contraseña anterior para crear una nueva. ésta es la única forma de cambiar la contraseña propia. Los administradores deberían pedir a los usuarios que cambiaran sus contraseñas regularmente y deberían establecer directivas de cuentas referidas a las restricciones en las contraseñas.

- ***Administrador de tareas (Task Manager)***: Proporciona una lista de los programas que se encuentran actualmente en funcionamiento, un resumen del use de CPU y memoria y una vista rápida de la forma en que cede programa, componente de programa o proceso del sistema está utilizando la CPU y los recursos de memoria. Se puede utilizar también el administrador de tareas para cambiar de un programa a otro y para parar un programa que no está respondiendo.

- ***Cancelar (Cancel)***: Cierra el cuadro de diálogo Seguridad de Windows.

Manejo de paquetería usando Network Monitor

Como un administrador, es importante mantener estadísticas del tráfico de red que se esta generando a través de tu red. No es necesario saber o estar familiarizado con cada simple paquete de red que se envía o que se recibe, pero lo que si se necesita saber que tipos de protocolos están fluyendo dentro de tu red. Monitorear la red permite que se tenga un mejor entendimiento de cómo es usado el ancho de banda. También te permite encontrar si usuarios están compartiendo archivos o programas, o si algún tipo de software malicioso como Troyanos esta trasmitiendo silenciosamente información a espaldas de los usuarios.

Microsoft ha dado una herramienta que puedes utilizar para supervisar tráfico de la red. Apropiadamente, la herramienta se llama Network Monitor. Hay actualmente dos diferentes versiones del monitor de la red que viene con los productos de Microsoft. La versión que viene con el Windows 2003 Server ® que es la versión descargable de Microsoft. Esta versión es similar a la versión completa, salvo que permite solamente que analices el tráfico enviado a o desde el servidor que esta corriendo el Monitor de Trafico. La versión completa de Network Monitor esta incluida con SMS Server. Permite que supervises cualquier máquina en tu red y que te determines qué usuarios están consumiendo la mayoría del ancho de banda. Puedes también utilizar la versión de SMS del Network Monitor para determinar qué protocolos están consumiendo mayor ancho de banda en la red, localizar routers de la red, y resolver los nombres de los dispositivos en direcciones físicas MAC.

Otra característica que tiene el Network Monitor versión de Windows es la capacidad de capturar, de corregir, y de retransmitir un paquete de red. Esta funcionalidad es utilizada por los hackers al realizar un ataque de reenvió de paquetes. La idea detrás de un ataque de reenvió de paquetes es que un hacker puede capturar un cierto paquete de información sensible, tal como un paquete de la autentificación de un usuario. Más adelante, si el hacker desea iniciar una sesión como algún otro usuario, podrían editar el paquete para cambiarle la dirección de origen y luego retransmitirlo.

Para instalar la versión básica de Network Monitor siga los siguientes pasos:

1. Abrir **Add/Remove Programs** en el **Control Panel** en menú **Start**.

2. Pulsar sobre **Add/Remove Windows Components.**

3. Seleccionar **Management and Monitoring Tools**, y pulsar sobre **Details.**

4. En esta ventana seleccionar la casilla **Network Monitor Tools** y luego hacer clic en **OK**.

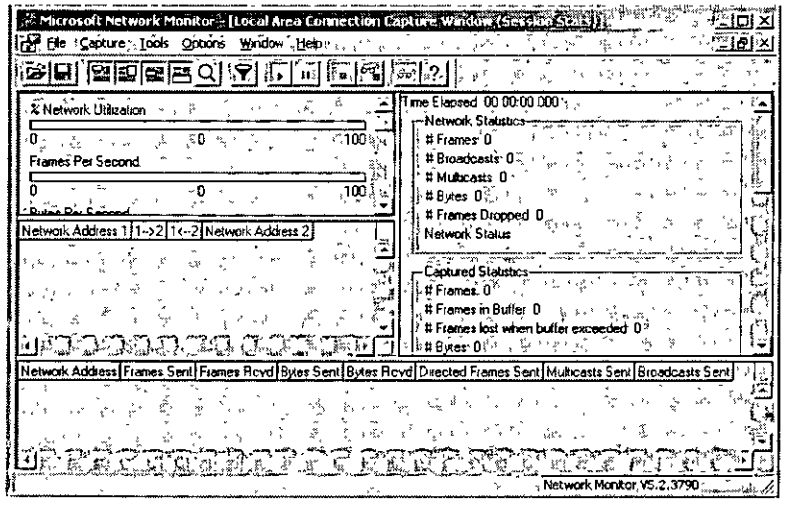
5. Hacer clic en **Next,** comenzará la instalación pero se requiere el disco Windows 2003 Server ® para continuar con la instalación.

6. Pulsar en **finish** y la instalación se abrá completado.

Inicio Network Monitor

Después de que el proceso de instalación se haya completado, ya se puede utilizar la herramienta **Network Monitor** que se encuentra en el menú **start,** y luego en **Administrative Tools**. Cuando el **Network Monitor** se abra aparecerá un cuadro de dialogo preguntando que selecciones la red de la cual deseas capturar los datos. Pulsa en **OK** y se verá la opción que hayas elegido en un cuadro de selección. Simplemente expandir el icono de **My Computer** y luego seleccionar la tarjeta de red que se quiere monitorear. Pulsar en **OK** para continuar.

En este punto, verás la pantalla principal del **Network Monitor**, que se muestra en la imagen, ahora **Network Monitor** no está capturando ningún dato. Se puede iniciar el proceso de recolección de datos en el momento que se desee. Antes de que inicie el proceso puede ser que se desee hacer un filtro de datos para tener una captura mas especializada.



La razón por la cual hacer un filtro es porque hay una enorme cantidad de tráfico en la red que fluye hacia y desde de la mayoría de los servidores. Puedes capturar fácilmente tanto tráfico que analizarlo se convierte en una tarea imposible. Para ayudar reducir en la cantidad de tráfico a analizar, **Network Monitor** permite que utilices los filtros. Hay dos tipos de filtros que se pueden utilizar: filtros de captura y filtros de exhibición.

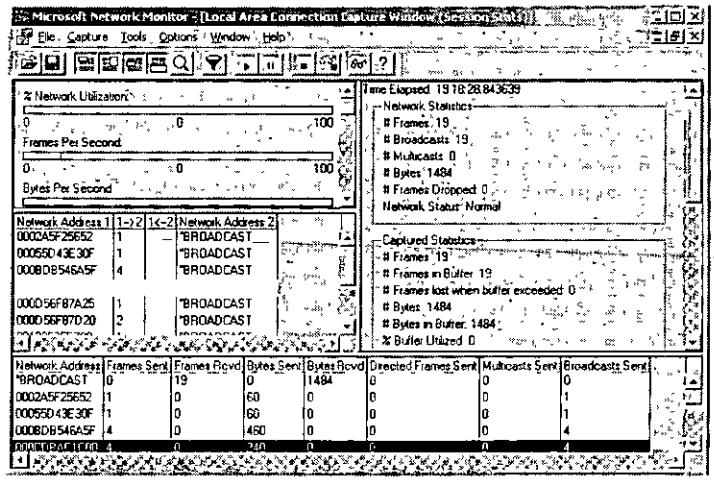
Los filtros de captura permiten que especifiques qué tipos de paquetes serán capturados para el análisis. Por ejemplo, puedes escoger que deseas solamente capturar los paquetes del protocolo HTTP. La ventaja principal a poner un filtro de captura es que cuando se

empieza a capturar información solo se filtrará lo establecido por lo que la información obtenida ocupara menos espacio de disco duro que si se captura todo el tráfico durante determinado tiempo.

Los filtros de exhibición trabajan semejantemente a los filtros de captura salvo que todo el tráfico de la red se captura. Filtras los datos que deseas analizar a la hora de análisis más bien que a la hora de captura. Estos filtros usan mucho mas espacio en el disco duro, pero se tendrá toda la captura de datos completa en caso de que decida analizar algo que originalmente se deseaba.

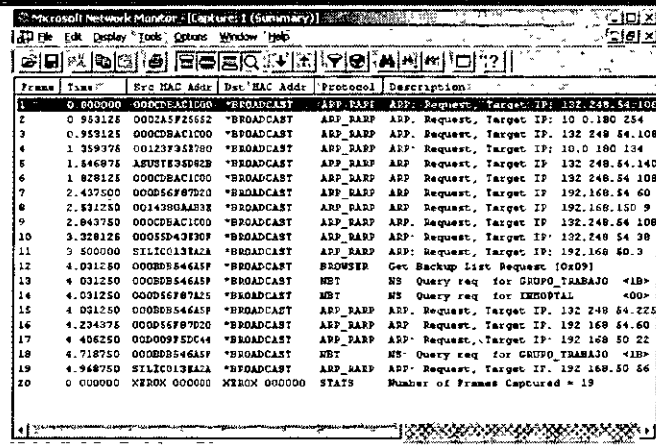
Capturando Paquetes

Si has decidido que deseas filtrar, los datos ya pueden ser capturados, seleccionar la opción del filtro del menú de **Capture**, para configurar el filtro. Si no, puedes comenzar el proceso de la captura seleccionando el comando del comienzo encontrado en el menú de **Capture**. Cuando has capturado los datos que deseas, entonces selecciona el comando de **Stop** del menú de **Capture.**



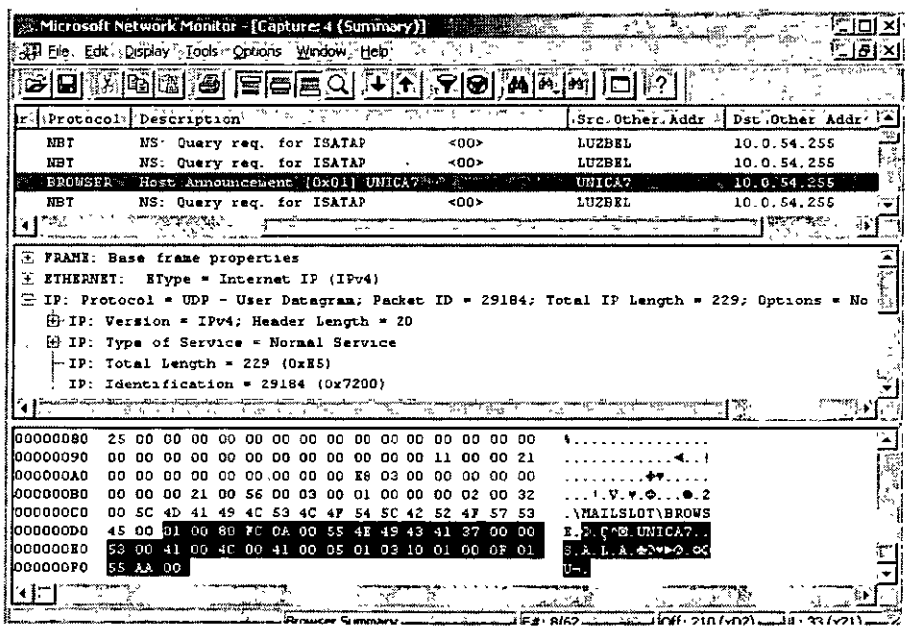
Analizando la captura

Para analizar los datos capturados, selecciona el botón **Display Captured Data** del menú de **Capture**.



La pantalla anterior muestra un resumen de todos los paquetes capturados en la secuencia que estos fueron capturados. Los datos que se muestran en la pantalla están filtrados con un filtro de tipo captura. Se puede aplicar aun un filtro de exhibición para mostrar información más específica. Seleccionar la opción de **Filter** en el menú.

Una vez localizado el paquete en el que se este interesado, seleccionarlo hacer doble clic en el paquete para ver mas detalles.



Como se puede ver en la figura, la pantalla del paquete se divide en tres secciones. En la parte de arriba es simplemente la ventana minimizada de la vista del resumen. Se puede usar esta sección para seleccionar un paquete diferente para analizarlo sin tener que regresar a la pantalla del resumen de los paquetes capturados.

La segunda sección contiene en formato de árbol el contenido descifrado del paquete. Por ejemplo, en la pantalla capturada se puede ver en la parte de arriba del árbol **FRAME: Base Frame Properties.** Si se expande esta porción del árbol se podrá ver la fecha y tiempo de cuando el **Frame** fue capturado, el número del **Frame** y la longitud del **Frame**.

La tercer sección contiene la información en bruto que contiene el Frame. En esta sección, la columna que se encuentra a la izquierda muestra la dirección base de los bytes en esa línea en formato hexadecimal. La sección de en medio muestra los datos hexadecimales reales que componen el Frame. Los códigos hexadecimales se muestran en pares. Para determinar la dirección de algún carácter en hexadecimal, empieza con la dirección base por línea, y luego cuenta la posición del carácter que se busca. Por ejemplo si la dirección base es 00000010, y el carácter que se esta buscando esta en la posición 12, entonces la dirección de carácter debe ser 0000001B.

La columna de la izquierda contiene la impresión del dato en formato decimal. Esta es probablemente la parte mas útil de la venta porque cualquier cosa que se ha transmitido en texto claro es claramente legible en esta columna. Por ejemplo, si un E-mail fue enviado en un formato sin encriptar y la transmisión fue capturada, se puede leer el contenido del mensaje en esta columna (asumiendo que se esta analizando el paquete que contenía esta información).

WINDOWS 2003 SERVER ®

Tema 2

Introducción a la Administración de Cuentas y Recursos

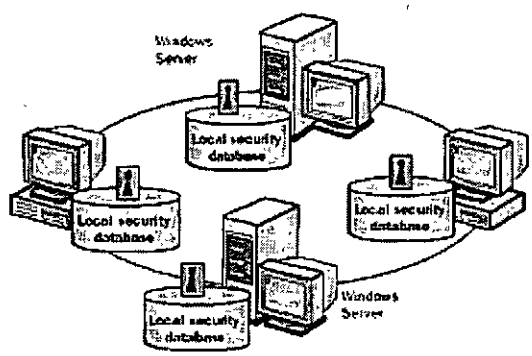
- Introducción a la Administración de cuentas y recursos
- La Familia Windows Server 2003 ®
- Instalar y configurar herramientas administrativas
- Crear cuentas de usuario
- Crear cuentas de equipo
- Crear una unidad organizativa

FLORES ALVAREZ LUIS ARMANDO
GUERRERO MARTÍNEZ EDSON ARMANDO

Introducción a la Administración de cuentas y recursos

Una red basada en Windows 2003 Server ® puede usar dos tipos de modelos, el modelo "Grupo de Trabajo (Workgroup)" o el modelo "Dominio (Domain)".

Modelo Workgroup



Un grupo de trabajo es una agrupación lógica de computadoras conectadas en red, que comparten recursos, como impresoras y archivos. A un grupo de trabajo se le conoce como red "punto a punto", porque todas las computadoras que participan en él pueden compartir recursos por igual sin la necesidad de un servidor dedicado.

Cada computadora del grupo de trabajo mantiene una base de datos de seguridad conocida como "local security database", que es una lista de cuentas de usuario e información de seguridad sobre recursos de la computadora en la que reside. Por lo tanto, la administración de cuentas de usuario y de seguridad de recursos en un grupo de trabajo, es descentralizada.

Las *desventajas* de utilizar un grupo de trabajo son:

- Un usuario debe tener una cuenta de usuario en cada computadora a la cual quiere obtener acceso.

- Cualquier cambio a una cuenta de usuario en cada computadora, como por ejemplo cambiar su contraseña o agregar una nueva cuenta de usuario debe ser hecho en cada computadora en grupo de trabajo. Si no se agrega una nueva cuenta de usuario a una computadora en el grupo de trabajo, el nuevo usuario no podrá iniciar sesión en dicha computadora y será incapaz de acceder a sus recursos.

- La compartición de dispositivos y archivos es manejada individualmente por cada computadora, y solo para los usuarios que tengan cuentas en cada computadora.

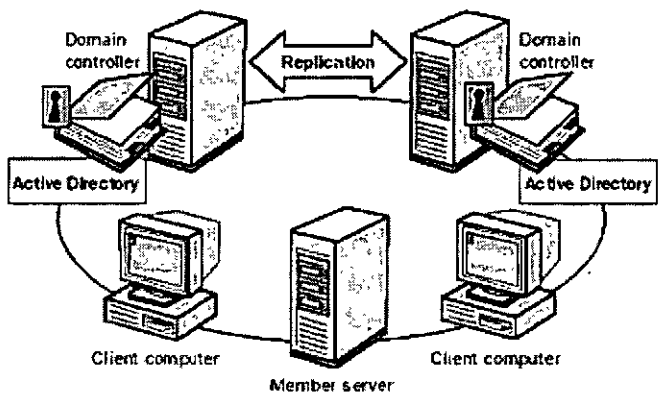
Un grupo de trabajo proporciona las siguientes *ventajas*:

- Un grupo de trabajo no requiere una computadora ejecutando Windows Server 2003 ® que almacene la información de seguridad de forma centralizada.

- Un grupo de trabajo es simple de diseñar e implementar. Un grupo de trabajo no requiere la gran planeación y administración que requiere un dominio.

- Un grupo de trabajo es conveniente para un número limitado de computadoras que se encuentren localizadas de forma cercana. (Un grupo de trabajo llega a ser un ambiente poco práctico en ambientes con más de 10 computadoras).

Modelo Domain



Un dominio es una agrupación lógica de computadoras en red que comparten una base de datos de directorio centralizada. Una base de datos de directorio, contiene cuentas de usuario e información de seguridad para el dominio, esta base de datos es conocida como el directorio y es una parte del Active Directory.

En un dominio, el directorio reside en computadoras configuradas como controladores de dominio (Domain Controllers). Un controlador de dominio es un servidor que controla todos los aspectos relacionados con la seguridad de los usuarios y el dominio. La seguridad y la administración están centralizadas. Solo las computadoras ejecutando Windows Server 2003 ® y Windows 2000 Server ® pueden ser promovidas a controladores de dominio.

Un dominio no hace referencia a una solo localidad o a un tipo específico de configuración red. Las computadoras en un dominio pueden compartir proximidad física en una pequeña LAN o pueden estar localizadas en diferentes partes del mundo, comunicándose a través de cualquier número de conexiones físicas (dial-up, ISDN, fibra óptica, etc.).

Los beneficios de un dominio son los siguientes:

- Un dominio permite la administración centralizada, debido a que toda la información de usuario está almacenada centralizadamente. Si un usuario cambia su contraseña, el cambio es automáticamente replicado en el dominio.

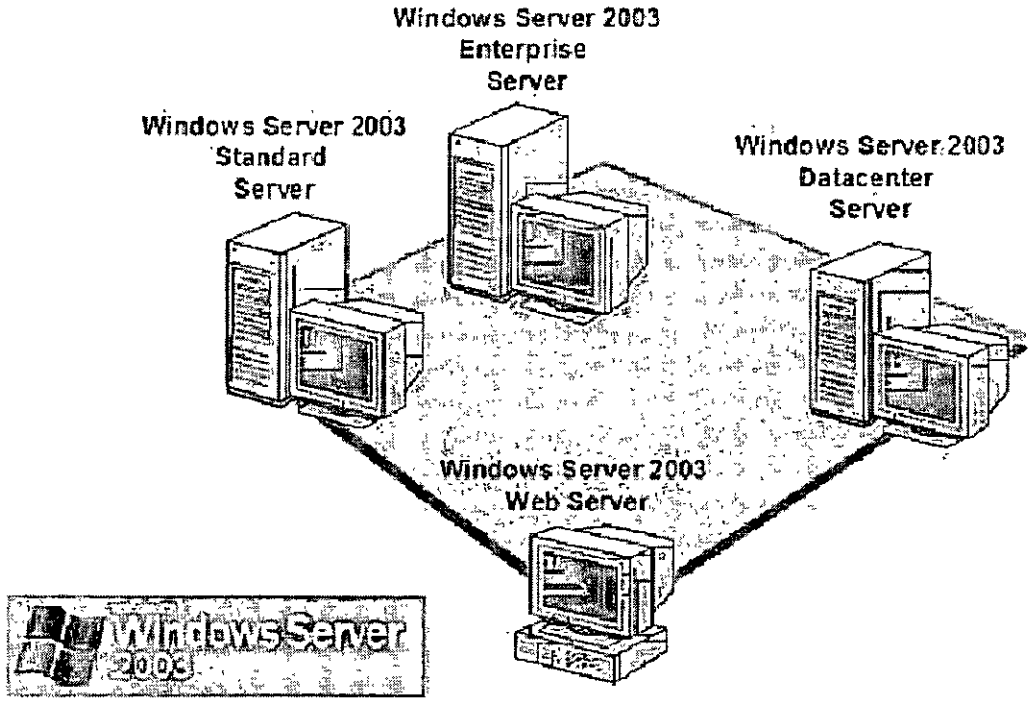
- Un dominio proporciona un proceso de inicio de sesión simple para que los usuarios accedan a los recursos de red como lo son archivos, impresoras y recursos de aplicaciones a los que tienen permiso. En otras palabras, un usuario puede iniciar sesión en una computadora y utilizar recursos de otra computadora en la red de acuerdo con los permisos apropiados en dichos recursos.

- Un dominio proporciona escalabilidad para que los administradores puedan crear redes muy grandes.

La Familia Windows Server 2003 ®

La familia de Windows 2003 Server ® esta compuesta por cuatro versiones que se adecuan de acuerdo a las necesidades de cada organización, las cuales son las siguientes:

- Standar Edition
- Enterprice Edition
- Datacenter Edition
- Web Edition



- MICROSOFT WINDOWS SERVER 2003 STANDARD EDITION ®. El sistema operativo servidor fiable ideal para satisfacer las necesidades diarias de empresas de todos los tamaños, proporcionando la solución óptima para compartir archivos e impresoras, conectividad segura a Internet, implementación centralizada de aplicaciones y un entorno de trabajo que conecta eficazmente a empleados, socios y clientes. Soporta hasta 4 procesadores y 4 Gb de Memoria RAM.

- MICROSOFT WINDOWS SERVER 2003 ENTERPRISE EDITION ®. La plataforma preferida tanto por las grandes compañías como por las de tamaño medio para implementar aplicaciones de forma segura, así como servicios Web. Integrándose en infraestructuras aportando fiabilidad, mejores rendimientos y un elevado valor empresarial, se presenta tanto en 32 como en 64 bit. Soporta hasta 8 procesadores, hasta 64 Gb de memoria RAM y permite clustering de hasta 8 nodos.

- MICROSOFT WINDOWS SERVER 2003 DATACENTER EDITION ®. Es el servidor escogido para aplicaciones críticas de negocio así como las consideradas de misión crítica, que exigen los más altos niveles de uptime, escalabilidad y fiabilidad. Sólo disponible a través del Datacenter Program de la mano de los fabricantes y proveedores de servicios líderes del mercado, se presenta en las versiones de 32 y 64 bit. y permite escalar por encima de las 8 vías o procesadores alcanzando hasta 64 procesadores en paralelo.

• MICROSOFT WINDOWS SERVER 2003 WEB EDITION ®. Optimizado específicamente para albergar y servir páginas web, manteniendo las funcionalidades esenciales que garantizan la fiabilidad, seguridad y facilidad de gestión características de Windows Server. Es la edición adecuada para implementar servidores web dedicados a bajo coste.

Para el correcto funcionamiento de cada una de ellas los requerimientos minimos recomendados de hardware son los siguiente:

-	*Server*	*Web Server*	*Enterprise Server*	*Datacenter*
CPU / RAM	2 CPU 4 GB	2 CPU 2GB	8 CPU 32 GB (x86) 64 GB (64-Bit)	8-64 CPU 64GB (x86) 512 GB (64-Bit)
Caracteristicas	**Nuevas Caracteristicas:** •NLBS •Personal Firewall	**Puede correr:** •IIS 6.0 •NLBS •DNS, DHCP, WINS **Limitaciones:** •No DC Promo •No Aplicaciones •No TS App •Mode	**All features from Standard plus:** •8-node Clustering •64-bit Version	**All features from Enterprise, plus:** •Datacenter program -Datacenter HCL -Maintenance •Multi-instance support

Windows Server 2003 Requerimientos del Sistema				
Requerimiento	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Velocidad de CPU mínima	133 MHz	133 MHz para arquitectura x86 733 MHz para arquitectura Itanium	400 MHz para arquitectura x86 733 MHz para arquitectura Itanium	133 MHz
Velocidad de CPU Recomendada	550 MHz	733 MHz	733 MHz	550 MHz
RAM Mínima	128 MB	128 MB	512 MB	128 MB
RAM Recomendada	256 MB	256 MB	1 GB	256 MB
RAM Máxima	4 GB	32 GB for para arquitectura x86 512 GB para arquitectura Itanium	64 GB para arquitectura x86 512 GB para arquitectura Itanium	2 GB
Soporte Multiprocesador SMP	Hasta 4	Hasta 8	Requerido 8 Mínimo Máximo 64	Hasta 2
Espacio Mínimo en Disco	1.5 GB	1.5 GB para arquitectura x86 2.0 GB para arquitectura	1.5 GB para arquitectura x86 2.0 GB para arquitectura	1.5 GB

Crear un dominio Windows 2003 Server® instalando Active Directory

I. Iniciar Active Directory Intallation wizard para crear:

Un nuevo controlador de dominio para un nuevo dominio
Un nuevo árbol de dominio
Un nuevo bosque o árboles de dominio

a) Iniciar sesión como Administrator

b) clic en **start** y luego en **Run**

c) En el cuadro de **Run** escribir **dcpromo** y luego **OK**

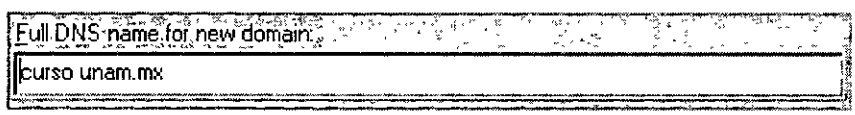
d) Clic en **Next** de **Active Directory Intallation wizard**

e) Leer la compatibilidad de sistemas operativos, dar clic **Next**

f) En la página **Domain Controler Type**, seleccionar **Domain controller for a new domain**, dar clic en **Next**

g) En la página de **Create a New Domain**, seleccionar **Domain in a new forest**, dar clic en **Next**

h) En la pagina de **New Domain Name**, en el cuadro de dialogo de **Full DNS name for new domain**, escribir ***dominio.unam.mx*** (domain nombre de dominio asignado)



i) En la pagina de **BIOS Domain Name** verificar que **DOMAIN** (domain es el nombre de dominio asignado) aparece, luego **Next**

j) En la pagina de **Database and Log Locations**, aceptar la localización predeterminada que nos da, clic **Next**

k) En la ventana **Shared System Volume**, aceptar la localización predeterminada dando clic en **Next**

l) En la ventana de **DNS Registration Diagnostic**, clic **Next**

m) En la ventana de **Permissions,** seleccionar **Permissions compatible only with Windows 2000 servers ® or Windows 2003 servers ®** dar clic en **Next.**

n) En la ventana **Directory services restore mode administrador password**, escribir contraseñas, clic **Next**

o) En la ventana **Summary**, verificar las opciones seleccionadas y dar clic en **Next**

p) Cuando la pagina **Completing the Active Directory Installation Wizard** aparezca, dar clic en **Finish**, y luego reiniciar la computadora.

II. Verificar la instalación del Active Directory

Después de haber completado la instalación del Active Directory, la segunda parte de la implementación requiere verificar que la instalación haya sido satisfactoria.

1. Verificar que los registros de recursos SVR hayan sido registrados en el DNS

a) Iniciar sesión como administrador

b) Abrir la con sola **DNS** de menú **Administrative Tools**

c) En el árbol de consola expandir la computadora (es decir el nombre de la computadora asignada), expandir **Forward Lookup Zone**, y después expandir ***dominio.unam.mx*** (donde dominio es el nombre del dominio asignado). Aparecerán los siguientes directorios bajo el dominio:

- _msdcs
- _sities
- _tcp
- _udp

Si los registros de recursos no aparecen se debe de abrir una ventana de línea de comandos, escribir **net stop netlogon** y después presionar **Enter**, escribir después **net start netlogon** y después presionar **Enter**. Esto se realiza para que los registros de recursos SRV sean dados de alta.

2. Verificar que el volumen de sistema compartido (SYSVOL) fue creado y compartido

a) En el cuadro **run** escribir **%systemroot%\sysvol** y dar clic en **ok.** Aparecerá una ventana que muestra el contenido del directorio **sysvol.** Se deberían ver los siguientes subdirectorios

- Domain
- Stating
- Stating Areas
- Sysvol (carpeta compartida)

b) Cerrar la ventana **Sysvol**

c) Abrir una ventana de línea de comandos

d) En la línea de comandos, escribir **net share** y después presionar **enter**. En la salida del comando **net share**, se deberá observar una entrada para **Sysvol** indicando que ha sido compartido

e) Cerrar la ventana de línea de comandos

3. Verificar que fue creada la base de datos y los archivos de registros asociados

a) En el cuadro **run,** escribir **%systemroot%\ntds** y presionar **enter**. Una ventana mostrara el contenido del directorio **Ntds**. Se deberían observar los siguientes subdirectorios:

- Drop
- Edb.
- Ntds.dit
- Res1

b) cerrar ventanas.

III. Convertir Zonas Primarias estandar de DNS a Zonas Integradas de Active Directory

1. Convertir la zona de búsqueda directa del dominio de zona primaria estándar a una zona integrada de Active Directory

a) Dar clic en **start**, seleccionar **Programs, Administrative Tools** y después dar clic en **DNS.**

b) En el árbol de consola, dar clic derecho en computadora, expandir **Forward Lookup Zone** y después dar clic en ***dominio.unam.mx*** (donde dominio en el nombre de dominio asignado).

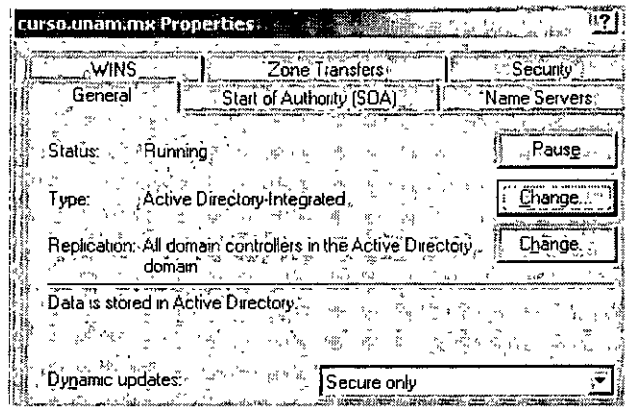
c) Dar clic derecho en ***dominio.unam.mx*** y después en **Propieties.**

d) En la pestaña **General** del cuadro de dialogo ***dominio.unam.mx*** **Properties** dar clic en **Change.**

e) En el cuadro de dialogo **Change Zone Type** dar clic en **Store the zone in Active Directory** y dar clic.

f) En el cuadro de dialogo **Change Zone Type**, dar clic **ok** para confirmar el cambio.

g) En la parte de **General** en **Dynamic Updates**, seleccionar **Secure only**, y después dar **ok.**



2. Convertir la zona de búsqueda inversa para una zona de red primaria estándar a una zona integrada de Active Directory

a) En el árbol de consola, expandir **Reverse Lookup Zone** y dar clic en **10.0.54.x subnet.**

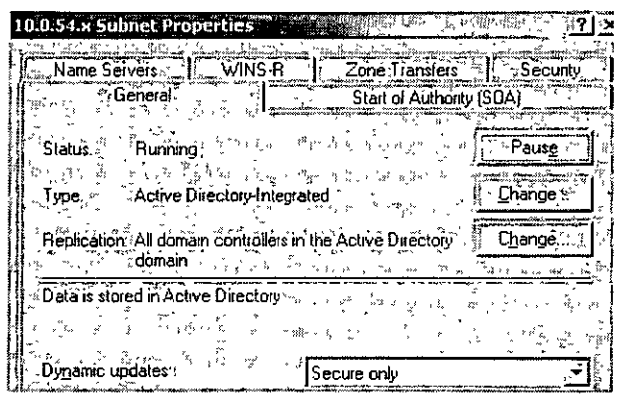
b) Dar clic derecho en **10.0.54.x subset** y después en **Properties.**

c) En la pestaña **General** del cuadro de dialogo **10.0.54.x Properties** dar clic en **Change.**

d) En el cuadro de dialogo **Change Zone Type** dar clic en **Store the zone in Active Directory** y luego **OK.**

e) En el cuadro de dialogo **Change Zone Type**, dar clic **ok** para confirmar el cambio.

f) En la parte de **General** en **Dynamic Updates**, seleccionar **Secure only**, y después dar **ok**.



g) Cerrar la consola **DNS**

- **Crear cuentas de usuario**

Las cuentas de usuario representan a una persona y se denominan principales de seguridad dentro del Directorio Activo, ya que son objetos del directorio a los que se les asignan automáticamente identificadores de seguridad para iniciar sesiones en la red y tener acceso a los recursos.
Una cuenta de usuario permite que un usuario inicie sesiones en equipos o dominios con una identidad que se puede autentificar y autorizar para tener acceso a los recursos del dominio. Cada usuario que se conecta a la red debe tener su propia cuenta usuario y su propia contraseña unica. Por lo tanto, una cuenta de usuario se utiliza para:

- Autentificar la identidad del usuario
- Autorizar o denegar el acceso a los recursos del dominio
- Administrar otros principales de seguridad
- Auditar las acciones realizadas con la cuenta de usuario

En Windows 2003 Server los usuarios pueden ser dos tipos:

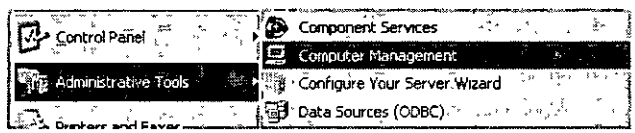
- **Usuarios Globales.** Estas cuentas se crean en equipos que son controladores de dominio y pueden usarse para conectarse a los dominios en que están creadas y a otros dominios en los que se confía.

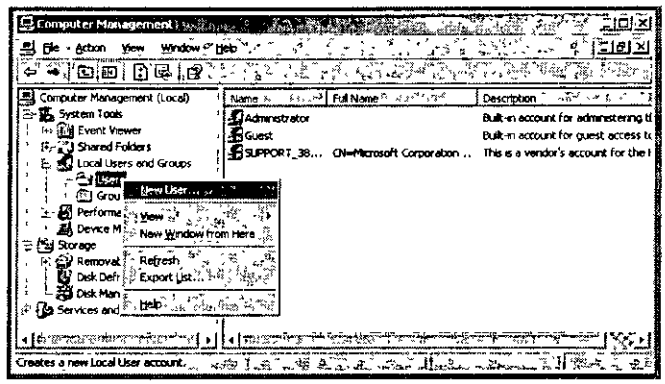
- **Usuarios locales.** Estas cuentas se crean en equipos que no son controladores de dominio y, por tanto, no pueden usarse para conectarse a ningún dominio.

Creando una Cuenta de Usuario Local

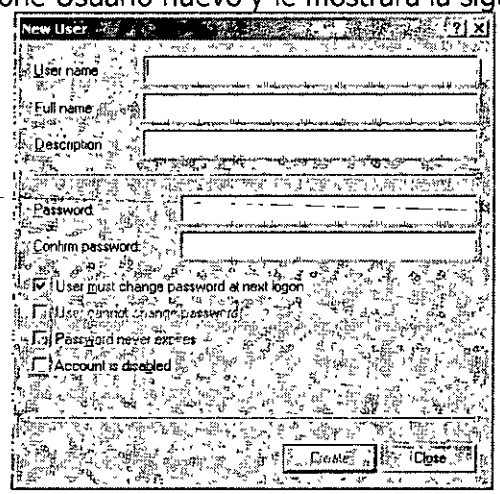
Para crear usuarios locales, siga los siguientes pasos:

1. Seleccione **Computer Management** de **Administrative Tools** del menú Inicio y vera la siguiente pantalla.





2. Pulse el botón izquierdo del ratón sobre el signo "+" que hay a la izquierda de Users y grupos locales, se encuentra en el panel izquierdo, y se desplegara su contenido, Usuarios y Grupos.
3. Pulse el botón izquierdo del ratón sobre Usuarios y, en el panel derecho, le mostrara los usuarios que hay dados de alta en el equipo.
4. Pulse el botón derecho del ratón sobre Usuarios para que muestre su menú contextual, seleccione Usuario nuevo y le mostrara la siguiente pantalla



5. Indique:

Nombre de Usuario: es el nombre que desea dar al usuario para conectarse, Nombre Completo: su nombre completo, es necesario seguir una norma ya que cuando se ordenen por el nombre completo será mas fácil su búsqueda.
Descripción del usuario: breve descripción del usuario
Password de Usuario: contraseña que utilizara el usuario para conectarse

- User must change password at next log on:

Con esta opción de obliga al usuario a cambiar su password al momento de iniciar sesión por primera vez.

- User cannot change password

El usuario no puede cambiar su password, necesita de la ayuda del administrador

- Password never expires

El password del usuario nunca expira por lo que el password siempre será el mismo

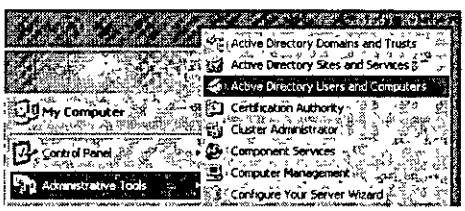
- Account is disable

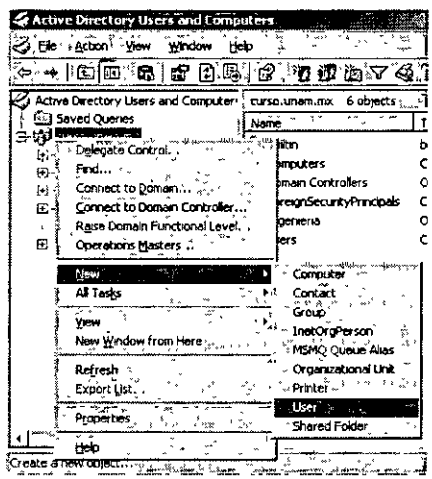
Cuenta deshabilitada, es importante esta opción cuando por ejemplo el usuario sale de vacaciones nadie podrá iniciar sesión bajo esta cuenta.

Creando una Cuenta de Usuario Global

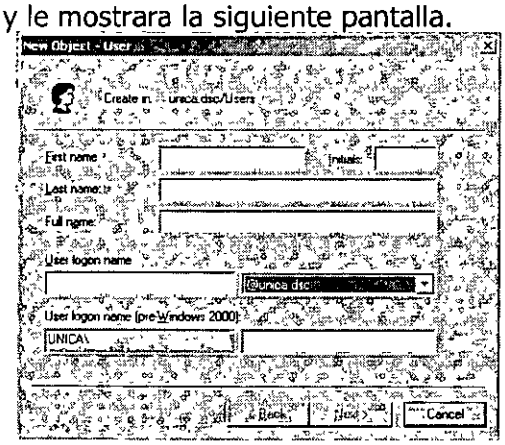
Para crear usuarios globales, siga los siguientes pasos:

1. Seleccione Usuarios y equipos de Active Directory de Herramientas administrativas del menú Inicio y vera la siguiente pantalla.



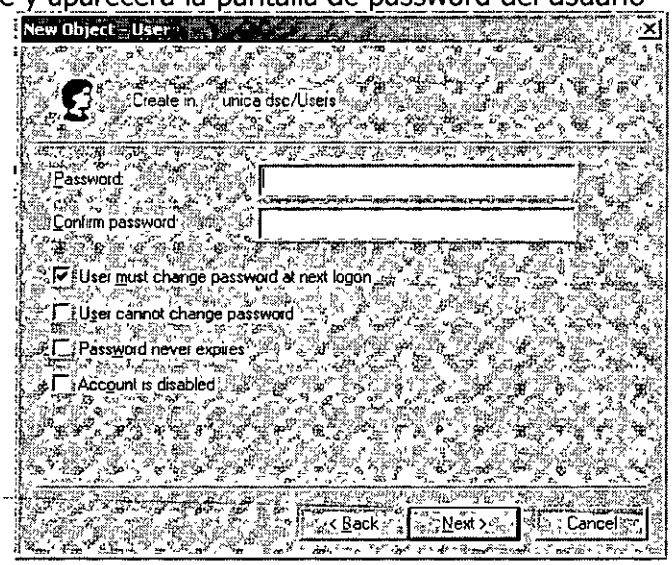


2. Pulse el botón izquierdo del ratón sobre el signo "+" que hay a la izquierda de Usuarios, se encuentra en el panel izquierdo, y se desplegara su contenido, Usuarios.
3. Pulse el botón izquierdo del ratón sobre Usuarios y, en el panel derecho, le mostrara los usuarios que hay dados de alta en el equipo.
4. Pulse el botón derecho del ratón sobre Usuarios para que muestre su menú contextual, seleccione Usuario nuevo y le mostrara la siguiente pantalla.



Nombre: Nombre de pila del usuario.
Iniciales: Iniciales del usuario.
Apellidos: Apellidos del usuario.
Nombre Completo: Nombre completo del usuario
Nombre de inicio de sesión de usuario: nombre con el cual el usuario iniciara la sesión. Del lado derecho se encuentra el dominio en el cual se creara el usuario.
Nombre de inicio de sesión pre-Windows 2000: para usuarios que iniciaran sesión desde equipos Windows 95/98/NT.

6. Pulse siguiente y aparecerá la pantalla de password del usuario



- User must change password at next log on:

Con esta opción de obliga al usuario a cambiar su password al momento de iniciar sesión por primera vez.

- User cannot change password

El usuario no puede cambiar su password, necesita de la ayuda del administrador

- Password never expires

El password del usuario nunca expira por lo que el password siempre será el mismo

- Account is disable

Cuenta deshabilitada, es importante esta opción cuando por ejemplo el usuario sale de vacaciones nadie podrá iniciar sesión bajo esta cuenta.

Cuenta de Equipo

Las cuentas de equipo representan a un equipo y se denominan principales de seguridad en el Active Directory, ya que son objetos del directorio a los que se asignan automáticamente identificadores de seguridad para iniciar sesiones en la red y tener acceso a los recursos.

Una cuenta de equipo permite iniciar sesiones en dominios con una identidad que se puede autentificar y autorizar para tener acceso a los recursos del dominio. Cada equipo que se conecta a la red debe tener su propia cuenta y se utiliza para:

- Autentificar la identidad del equipo.
- Autorizar o denegar el acceso a los recursos del dominio.
- Administrar las acciones realizadas con la cuenta de equipo.
- Auditar las acciones realizadas con la cuenta de equipo

A una cuenta de equipo se le puede conceder permisos y derechos para el dominio donde se ha creado la cuenta. Se crea en el directorio activo y se guarda en equipos que disponen de Windows 2003 Server ® que sean controladores de dominio.

En el proceso de instalacion de Active Directory se han creado dos carpetas para almacenar las cuentas de equipo, lo que no significa que no se puedan almacenar en otras carpetas. Las carpetas en cuestión son: Domain Controllers, en esta carpeta se almacenarán todas las cuentas de los equipos que sean controladores de dominio, y Computers, en esta carpeta se almacenarán todas las demás cuentas de equipos.

Creando una Cuenta de Equipo

Para crear cuentas de equipo, siga los siguientes pasos:

1. Seleccione **Active Directory Users and Computers** de **Administrative Tools** del menú **Start** y vera la siguiente pantalla.

2. Pulse el botón izquierdo del ratón sobre el signo "+" que hay a la izquierda de Computers o Domain Controllers, se encuentra en el panel izquierdo, y se desplegara su contenido y en el panel derecho, le mostrara las cuentas de equipo que hay.
4. Pulse el botón derecho del ratón sobre Computers o Domain Controllers para que muestre su menú contextual, seleccione New y Computer le mostrara la siguiente pantalla.

Computer Name: Nombre del equipo.
Computer Name (Windows 200): si el equipo a unir tiene un sistema operativo anterior a Windows 2000.
User or Group: nombre de usuario o grupo que podrá unir el equipo al dominio.

5. Al finalizar con esta información presione sobre Next y aparecerá una ventana en donde se indicara el nombre de identificación único que se encuentra en la BIOS del sistema.

6. Después pulse sobre Next y aparecerá la pantalla del Summary y de clic sobre Finalizar.

- Crear una unidad organizativa

Las unidades organizativas son contenedores de Active Directory en los que puede colocar usuarios, grupos, equipos y otras unidades organizativas. Puede crear unidades organizativas que reflejen la estructura funcional o empresarial de su organización. Cada dominio puede implementar su propia jerarquía de unidad organizativa. Si su organización contiene varios dominios, puede crear en cada uno estructuras de unidad organizativa que sean independientes de las estructuras de los otros dominios.

Una unidad organizativa es la unidad o ámbito más pequeño al que puede asignar valores de Directiva de grupo o delegar autoridad administrativa. Con las unidades organizativas puede crear en un dominio contenedores que representan las estructuras jerárquicas y lógicas de su organización. Puede hacerlo como ayuda para la administración de la configuración y el uso de cuentas y recursos basándose en su modelo organizativo.

Las unidades organizativas pueden contener usuarios, grupos, equipos, impresoras y carpetas compartidas, así como un número ilimitado de otras unidades organizativas, pero no pueden contener objetos de otros dominios.

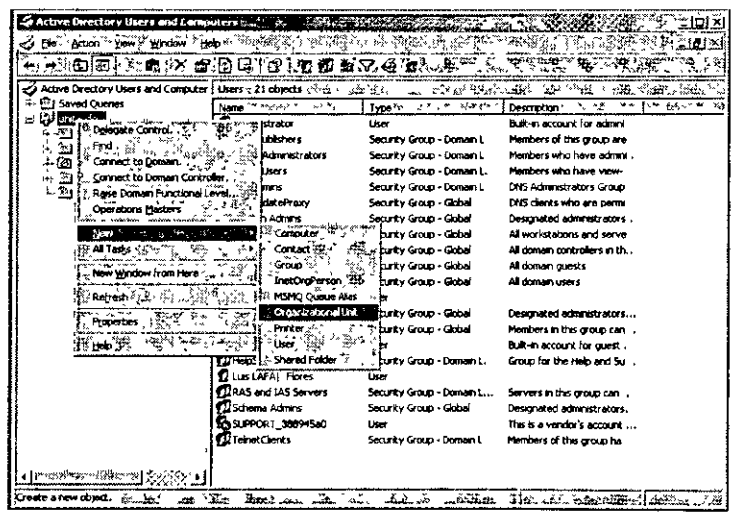
1. Haga clic en **Inicio**, seleccione **Herramientas administrativas** y, a continuación, haga clic en **Usuarios y equipos de Active Directory**.

2. Utilice uno de los pasos siguientes:

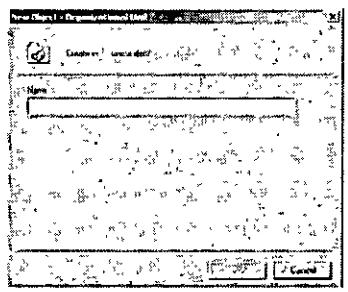
a) Haga clic con el botón secundario del *mouse* (ratón) en un objeto de dominio o unidad organizativa en el que desea crear las unidades organizativas, seleccione **Nuevo** y, a continuación, haga clic en **Unidad organizativa**.

b) Haga clic en **Crear una unidad organizativa nueva** en la barra de herramientas.

c) En el menú **Acción**, seleccione **Nueva** y, a continuación, haga clic en **Unidad organizativa**.



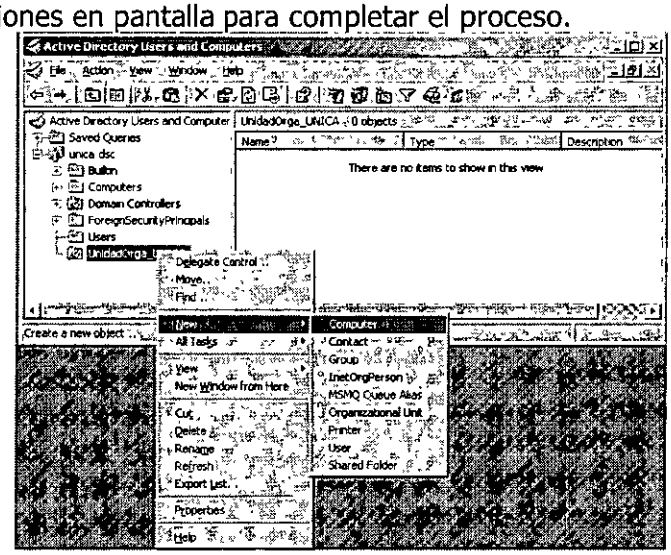
3. En el cuadro **Nombre**, escriba un nombre descriptivo para el objeto nuevo y, después, haga clic en **Aceptar**. Se crea e inserta en la lista un icono con el nombre correspondiente.



4. Agregue otros objetos a la unidad organizativa, como usuarios, equipos, grupos y otras unidades organizativas:

a) Haga clic con el botón secundario del *mouse* en la unidad organizativa recién creada, seleccione **Nuevo** en el menú contextual y haga clic en el nombre del objeto que desee agregar a la unidad organizativa.

b) Siga las instrucciones en pantalla para completar el proceso.



Crear Cuentas de Usuario utilizando un Sufijo de Nombre Principal de usuario Alterno

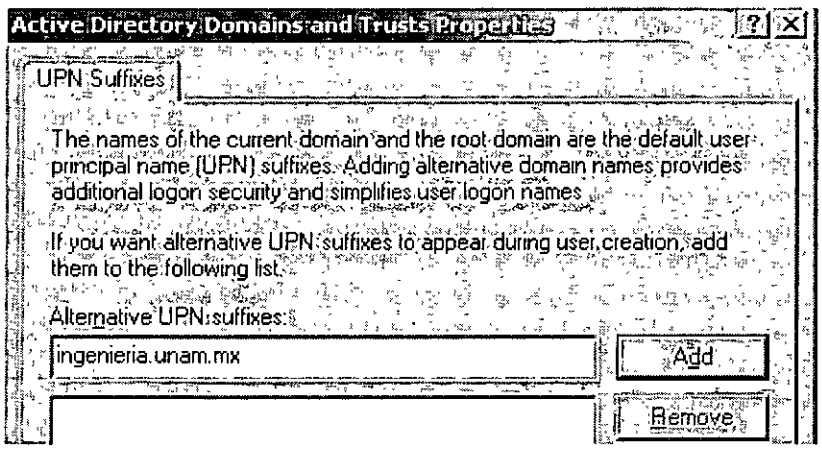
1. Crear el sufijo de nombre principal ingenieria.unam.mx

a) Iniciar sesión como Administrador

b) Abrir Active Directory Domain and Trust del menú Administrative Tools

c) En el árbol de consola, dar clic derecho en Active Directory Domain and Trust después dar clic en Properties

d) En el cuadro Alternative UPN Suffixes del cuadro de dialogo Active Directory Domain and Trust Properties escribir ingenieria.unam.mx y dar clic en Add y después dar clic en OK



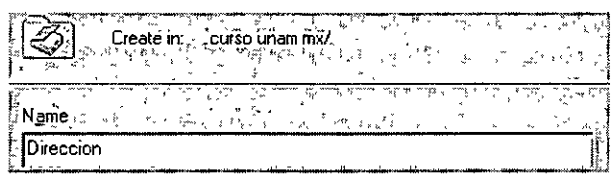
e) Cerrar Active Directory Domain and Trust

2. Dentro del dominio.unam.mx crear la OU: Dirección

a) Abrir Active Directory Users and Computers del menú Administrative Tools

b) En el árbol de consola, dar clic derecho en domain.unam.mx, apuntar a New y después dar clic en Organizacional Unit

c) En el cuadro Name del cuadro de dialogo New Object-Organizacional Unit escribir Ingeniería y después dar clic en OK



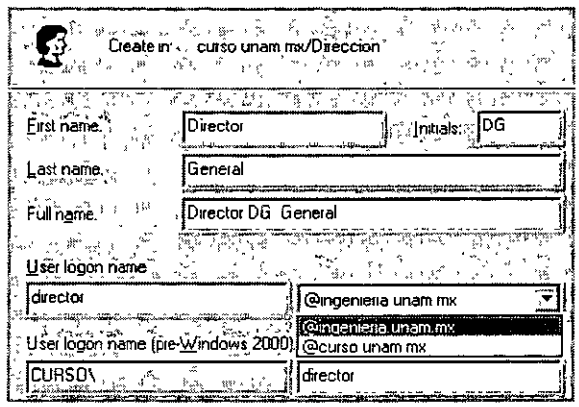
3. Dentro de la OU Ingeniería crear una cuenta de usuario con las siguientes propiedades: Full Name: Director General y User logon name: director@ingenieria.unam.mx

a) En el árbol de consola, dar clic derecho en domain.unam.mx y después dar clic en Ingeniería

b) Dar clic derecho en Ingeniería, apuntar a New y después User

c) En la pagina New Object – User, escribir Director General en los cuadros Full Name y User logon name.

d) Dar clic en la lista de los sufijos de nombre principal de usuario y dar clic en @ingenieria.unam.mx y después dar clic en Next



e) Ingresar contraseña dar clic en Next y después en Finish

f) Cerrar Active Directory User and Computers

4. Iniciar sesión utilizando el nombre de inicio de sesión de usuario director@ingenieria.unam.mx para verificar que la cuenta funcione y después cerrar sesión.

WINDOWS 2003 SERVER ®

Tema 3

Administración de Cuentas de Equipo y Usuario

- Modificar propiedades de cuentas de equipo y usuario
- Activar y desactivar cuentas de equipo y usuario
- Crear una plantilla de cuenta de usuario
- Ubicar cuentas de equipo y usuario en directorio activo
- Guardar consultas
- Restablecer cuentas de equipo y usuario
- Mover objetos de dominio

FLORES ALVARES LUIS ARMANDO
GUERRERO MARTINEZ EDSON ARMANDO

Modificar propiedades de cuentas de equipo y usuario

Un conjunto de propiedades predeterminadas es asociado a cada cuenta de usuario de dominio que se crea. Después de que se crea una cuenta de usuario de dominio, se pueden configurar propiedades personales y de cuenta, opciones de inicio de sesión y configuraciones de marcado.

El cuadro de diálogo **Properties** contiene información acerca de cada cuenta de usuario. Esta información está almacenada en **Active Directory**. Mientras más completa sea la información será mucho más fácil la búsqueda de los usuarios en **Active Directory**.

Para modificar usuarios globales o hacerlos miembros de un grupo, siga los siguientes pasos:

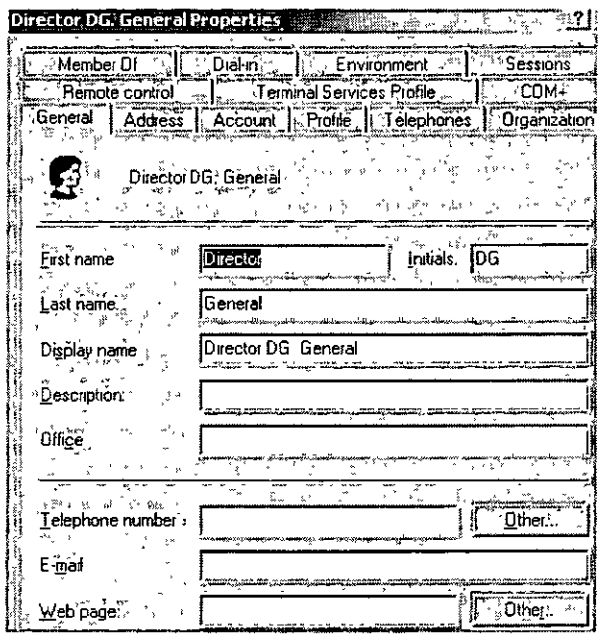
1. Modificar usuarios

a) Iniciar cuenta como administrador.

b) Abrir **Active Directory Users and Computers** del menu de **Administrative Tools.**

c) Desplegar el contenido del **dominio.unam.mx**, y situarse sobre **Users** o alguna otra Unidad Organizativa en donde tenga el usuario a modificar.

d) Seleccione el usuario a modificar, dar clic derecho sobre el usuario e ir a la opción de **Propierties.**



Aparecerá la pantalla en donde podremos ingresar o modificar la información completa del usuario

- **General.** Información personal del usuario: nombre completo, iniciales, e-mail, etc.
- **Address.** Información concerniente a la dirección completa del usuario.
- **Account**. Descripción de la cuenta, aquí se administra la cuenta del usuario, es una pantalla muy importante ya que aquí se pueden encontrar características de cuenta como nombre de la cuenta, dominio, desde que equipo se puede utilizar la cuenta, cuando expira, el tiempo de vida de la cuenta, etc.
- **Profile.** Permite asignar perfiles al usuario, una secuencia de comandos al iniciar sesión.
- **Telephones.** Teléfonos en donde se puede localizar al usuario.
- **Organization.** Si los usuarios forman parte de alguna organización.
- **Remote control.** Configurar el control remoto de los servicios de Terminal Server del usuario.
- **Terminal Services Profile.** Configurar los servicios de Terminal Server del usuario.
- **COM+.** Indicar conjuntos de particiones COM+ que se pueden asignar al usuario.
- **Dial-In.** Configurar el uso de Acceso telefónico a redes del usuario.
- **Enviroment.** Configurar el inicio de sesión de los Servicios de Terminal Server del usuario.
- **Sessions.** Configurar y administrar el uso de las sesiones del usuario.
- **Member Of**. Aquí se permite asignar a que grupos puede pertenecer el usuario.

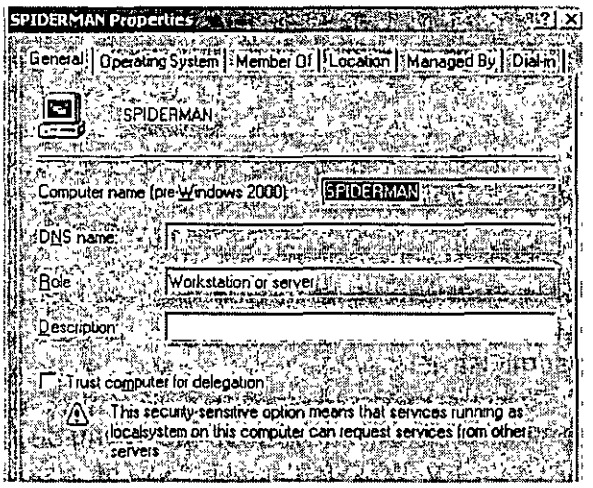
2. Modificar propiedades de cuentas de equipo

a) Iniciar cuenta como administrador.

b) Abrir **Active Directory Users and Computers** del menu de **Administrative Tools**.

c) Desplegar el contenido del **dominio.unam.mx**, y situarse sobre **Computers** o alguna otra Unidad Organizativa en donde tenga las cuentas de equipo a modificar.

d) Seleccione la cuenta de equipo a modificar, dar clic derecho sobre la cuenta de equipo e ir a la opción de **Propierties.**



Aparecerá la pantalla en donde podremos ingresar o modificar la información completa del equipo

- **General.** Información de nombre de equipo, nombre DNS, función, descripción y confiar el equipo a otra delegación
- **Operating System.** Nombre del sistema operativo del equipo, versión y último service pack.
- **Member of.** Indica los grupos a los que pertenece el equipo, aquí podemos agregar el equipo a otros grupos.
- **Location.** Aparecerá una pantalla en la cual podrá indicar el lugar donde se encuentra el equipo.
- **Manager By.** Aquí podremos indicar el usuario o grupo responsable de la administración de este grupo y sus datos, se puede modificar, borrar o agregar administrador.
- **Dial-In.** Se podrá configurar el uso del Acceso telefónico a redes del equipo.

Activar y deshabilitar cuentas de equipo y usuario

Para activar o desbloquear cuentas de equipo y usuario se necesita realizar los siguientes pasos

1. Activar y deshabilitar cuentas de equipo

a) Iniciar cuenta como administrador.

b) Abrir **Active Directory Users and Computers** del menu de **Administrative Tools**.

c) Desplegar el contenido del **dominio.unam.mx**, y situarse sobre **Computers** o alguna otra Unidad Organizativa en donde tenga las cuentas de equipo a activar/deshabilitar.

d) Seleccione la cuenta de equipo, dar clic derecho, y escoger **Enable/Disable** para habilitarla/deshabilitarla respectivamente

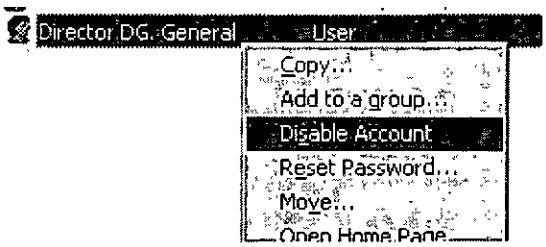
2. Activar y deshabilitar cuentas de usuarios

a) Iniciar cuenta como administrador.

b) Abrir **Active Directory Users and Computers** del menú de **Administrative Tools**.

c) Desplegar el contenido del **dominio.unam.mx**, y situarse sobre **Users** o alguna otra Unidad Organizativa en donde tenga las cuentas de usuarios a activar/deshabilitar.

d) Seleccione la cuenta de usuario, dar clic derecho, y escoger **Enable/Disable** para habilitarla/deshabilitarla respectivamente.



Crear una plantilla de cuenta de usuario

Las plantillas de cuentas de usuario nos proporcionan una manera abreviada para crear nuevas cuentas de usuario. Son cuentas de usuario estándar creadas con las propiedades que se aplican a usuarios con necesidades comunes. Por ejemplo, si todo el personal administrativo necesita ser miembro de un grupo especifico, podemos crear una plantilla que le provea de la pertenencia a ese grupo. Para utilizar una plantilla y crear con ella una cuenta de usuario, basta con copiar la cuenta plantilla (cualquier cuenta) y asignar un nombre de usuario y una contraseña para el nuevo usuario. Las siguientes opciones se convierten en propiedades de la nueva cuenta de usuario:

- Descripción.
- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
- El usuario no puede cambiar la contraseña.
- La contraseña nunca caduca
- Grupos.
- Perfil.

- Horas de inicio de sesión (sólo controladores de dominio).
- Iniciar desde (sólo controladores de dominio).
- Cuenta (sólo controladores de dominio).
- Marcado.

Nota: Los derechos y permisos concedidos a una cuenta de usuario individual no se copian.

Sugerencias para crear plantillas:

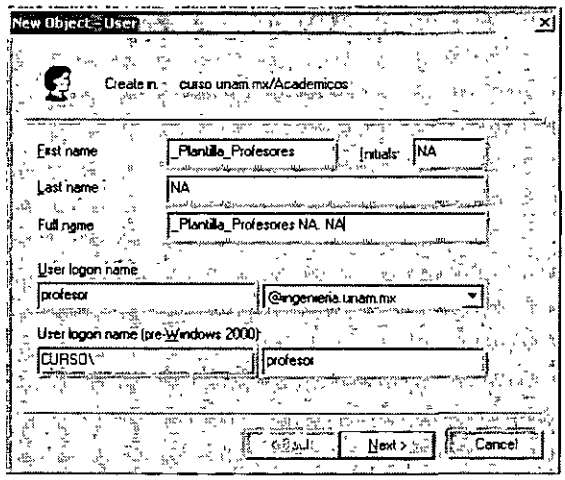
- Crear una plantilla para cada clasificación de empleado, por ejemplo, personal de ventas, contables, jefes, etc.
- Si normalmente tenemos usuarios temporales o durante poco tiempo, crearemos una plantilla con horas de inicio de sesión limitadas, especificaciones de estaciones de trabajo y otras restricciones necesarias.
- Es recomendable que cada nombre de plantilla comience con un carácter no alfabético, por ejemplo un carácter de subrayado (_), de esta forma las plantillas siempre aparecerán al principio de la lista de la ventana "Administrador de Usuarios".

1.- Crear una plantilla de usuario con atributos específicos

a) En el árbol de consola, dar clic derecho en ***domain.unam.mx*** y después dar clic en Ingenieria.

b) Dar clic derecho en Ingenieria, apuntar a **New** y después **User.**

c) En la pagina **New Object – User**, escribir _Plantilla_Profesores en el campo **First name** y llenar la información necesaria, como se muestra a continuación.

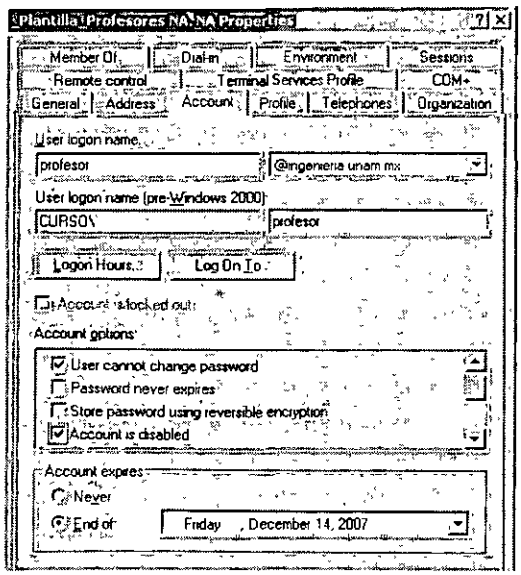


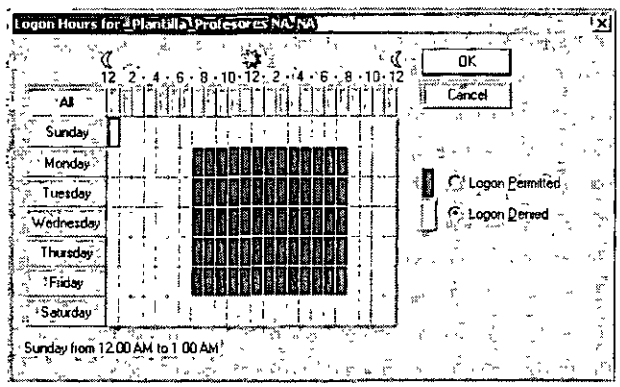
d) En la siguiente ventana colocar una contraseña valida, además de verificar que las opciones de la cuenta de preferencia estén deshabilitadas.

e) Confirmar y dar clic en **Next.**

f) Aparecerá creada una cuenta, la cual se seleccionará, dar clic derecho sobre ella e ir a **Properties**

g) En esta parte de las propiedades de la cuenta es donde definiremos los parámetros de nuestra plantilla, los valores de configuración de la cuenta que estamos editando serán los valores que tomaran las cuentas que realizaremos a partir de esta. Para este ejemplo editar la información de **Account** además de **Member of** y agregarla a un grupo que tengamos creado





h) Después de fijar los valores de la plantilla, dar **OK** veremos que tenemos nuestra plantilla lista, en este caso aparece con en estado de **disabled**.

Para utilizar la plantilla de cuenta y crear con ella una cuenta de usuario, basta con copiar la plantilla.

a) Seleccionamos la plantilla que deseamos copiar damos clic derecho, hacer clic en **Copy**.

b) Aparecerá la ventana de datos de la nueva cuenta.

c) Escribir un nombre de usuario y una contraseña para la nueva cuenta; luego hacer clic en **Finish**.

d) Para ver las propiedades con que fue creada esta cuenta, dar clic derecho sobre ella y verificar que los atributos que presenta con los establecidos en la plantilla.

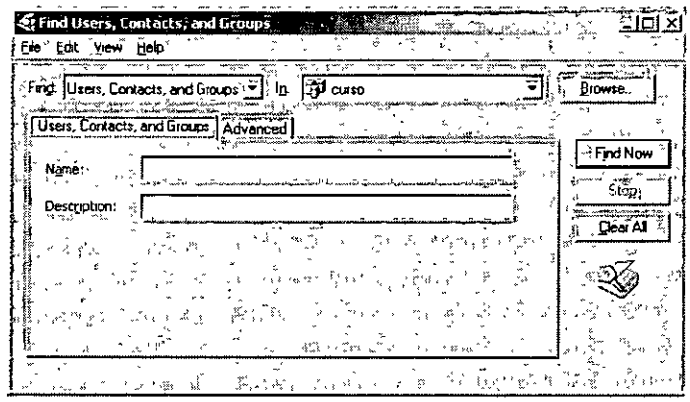
Ubicar cuentas de equipo y usuario en directorio activo

Una vez que ya tenemos creadas cuentas de usuarios, cuentas de equipos, grupos y unidades organizativas ahora podemos buscarlos dentro del **Active Directory**. En la medida en que crezca nuestro **Active Directory** la búsqueda de objetos será cada vez más compleja. Para ello existe la herramienta de **Find** en donde se pueden realizar diversas consultas de búsqueda de objetos tan simples o tan complejas, según se requieran.

- Para ubicar una cuenta de equipo y usuario dentro del **Active Directory**:

a) Abrir la consola de **Active Directory Users and Computers.**

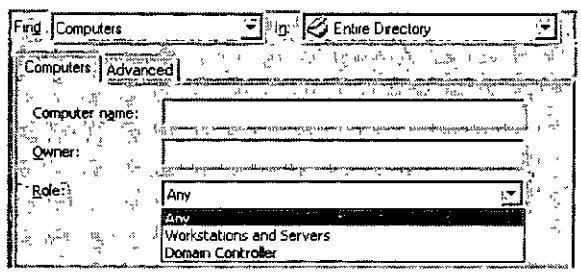
b) Seleccionar el dominio en donde se quiera realizar la búsqueda del objeto e ir al menú de **Action**, en donde se encuentra la opción **Find**, elegirla y entonces abrirá la siguiente ventana.



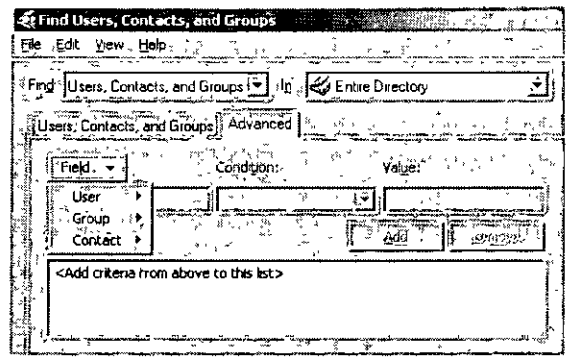
c) En esta ventana podemos realizar las búsquedas de los objetos del **Active Directory** como Usuarios, Contactos, Grupos, Equipos, Impresoras, Carpetas Compartidas, etc. En el menú desplegable que dice **Find** escogemos el objeto y en el menú desplegable de **In** escogemos donde lo vamos a buscar, puede ser dentro de un solo dominio o dentro de todo el **Active Direcrory**.

d) Cada uno de los objetos del **Active Directory** tiene diferentes atributos por los que podemos localizarlos, por ejemplo en la pantalla anterior teníamos seleccionado **Users, Contacts and Groups,** estos los podemos buscar por **Name** o **Description**; otro objeto que podemos localizar dentro del directorio activo son los equipos que a su vez tienen atributos diferentes por los que podemos localizarlos como **Computer name,**

Owner, Role. Cuando especificamos el o los valores solo es cuestión de dar clic en el botón de **Find Now** para que comience la búsqueda.



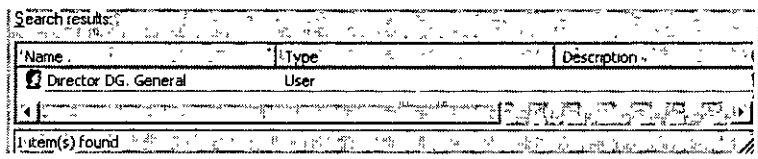
e) Todos los objetos que podemos localizar dentro del **Active Directory** los podemos encontrar por medio de una búsqueda avanzada, en la pestaña de **Advanced** podemos realizar una búsqueda mas especifica, aquí podemos hacer búsquedas con condiciones y patrones de búsqueda con valores específicos. Para el caso de **Users, Contacts, and Groups** podemos especializar la búsqueda de un usuario seleccionando en el campo **Field** la opción **User** y aparecerá un menú desplegable de todos los atributos de **User**.



f) Al seleccionarlo se habilitara el menú desplegable de **Condition** en donde se tienen las opciones de **Starts with, Ende with, Is (exactly), Is not, present y not present** con estas opciones limitamos el rango de búsqueda, al seleccionar uno podemos introducir su respectivo valor de búsqueda en el campo **Value**.

g) Cuando introducimos el valor de coincidencia hay que agregarla a la lista de condiciones esto se realiza mediante el botón **Add**.

h) Después solo iniciar la búsqueda **Find Now**, y si hay coincidencia con algún objeto del Active Directory en la parte inferior de la ventana aparecerán los resultados si tuvo éxito la búsqueda.



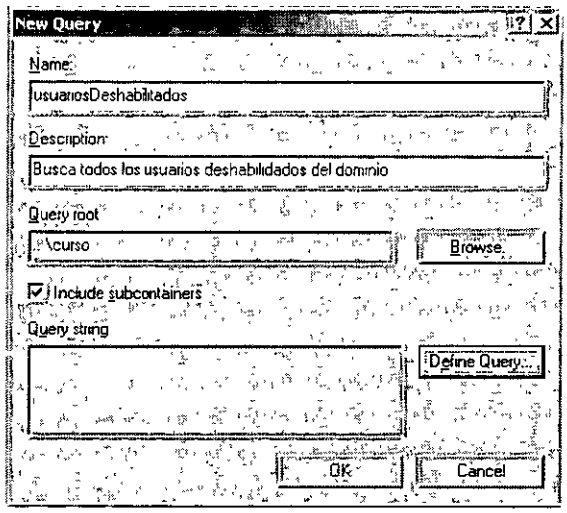
Guardar consultas

Otra manera de realizar consultas y guardar las consultas realizadas para poderlas utilizar posteriormente es desde la opción **Saved Queries** de la utilizad **Active Directoy Users and Computers**. Para ello siga los siguientes pasos:

a) Seleccione Active **Directoy Users and Computers** de **Administrative Tools** del menú **Start** y vera la pantalla principal de la utilidad.

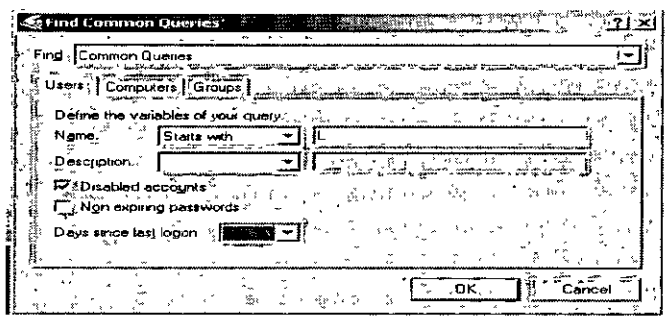
b) Pulse el botón izquierdo del ratón sobre la carpeta **Saved Queries** para ver si hay alguna consulta ya creada.

c) Pulse el botón derecho del ratón sobre la carpeta **Saved Queries** para que muestre su menú contextual, seleccione **New**, elija **Query** y le mostrara la siguiente pantalla:



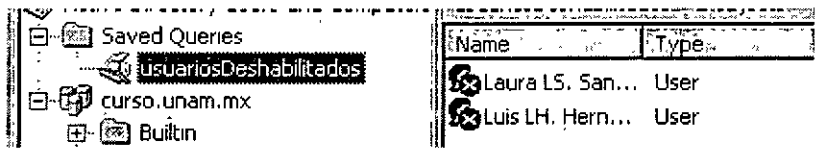
En ella se encuentran los campos de **Name** en donde se especificara el nombre con que se guardara la consulta, **Description** donde podrá escribir una breve descripción de lo que hace la consulta, además de **Query root** en donde seleccionamos la carpeta raiz del directorio activo o podemos cambiarla y además de activar la casilla de incluir subdirectorios.

d) Pulsar sobre **Define Query** nos dará la ventana **Find Common Queries**, en esta ventana tenemos acceso a las consultas comunes del **Active Directory**. En el menú desplegable se encuentran las opciones de Usuarios, Contactos, Grupos, Equipos, Impresoras, Carpetas Compartidas, etc.



e) Además de elegir que tipo de consulta le podemos hacer búsquedas por nombre o descripción. Si aparece habilitada o deshabilitada, si expira o no, y cuantos días tiene desde su último ingreso al sistema.

f) Al terminar de personalizar la búsqueda pulsar **OK** y guardar la búsqueda aparecerá en la ventana **Active Directoy Users and Computers de Administrative Tools** con los resultados arrojados por la búsqueda.



g) Las búsquedas pueden ser organizadas en carpetas según su ámbito. Cuando se desee utilizar una consulta guardada solo hay que seleccionarla, pulsar clic derecho sobre ella y escoger del menú emergente la opción de **Refresh** y se ejecutara la consulta.

Restablecer cuentas de equipo y usuario

Mover objetos de dominio

En Windows 2003 Server dentro del **Active Directory** se tiene la posibilidad de operar con facilidad los objetos del Directorio Activo y moverlos con gran facilidad. La administración del Directorio Activo de esta forma se hace más fácil.

- Para mover los objetos dentro del Directorio Activo solo es necesario realizar los siguientes pasos:

1. Seleccione Active **Directoy Users and Computers** de **Administrative Tools** del menú **Start** y verá la pantalla principal de la utilidad.

2. Pulse el botón derecho del ratón sobre el objeto de dominio que se desea mover.

3. Aparecerá el menú contextual del la cuenta, aquí aparecerá la opción **Move** seleccionar.

4. Entonces tendremos la ventana de selección del destino del objeto del **Active Directory.**

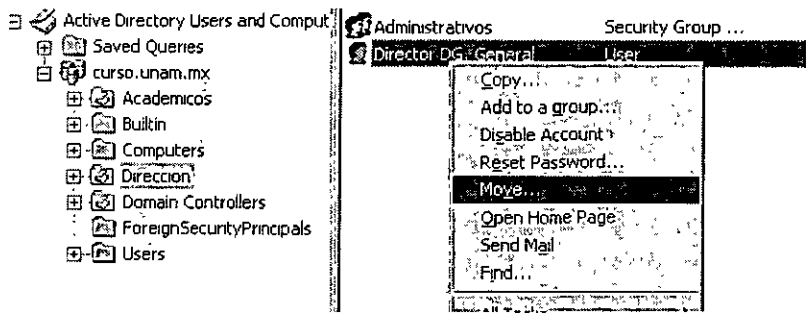
5. Vemos que aparece todo el dominio por lo que puede moverse al lugar que se desee.

Ejemplo.

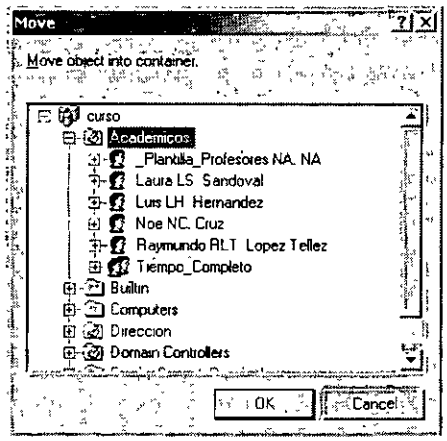
Vamos a mover una cuenta de una Unidad Organizativa a otra, en este caso moveremos la cuenta Director de la Unidad Organizativa Dirección a la Unidad Organizativa Académicos.

a) Seleccione Active **Directoy Users and Computers** de **Administrative Tools** del menú **Start** y verá la pantalla principal de la utilidad.

b) Expandimos la unidad organizativa Dirección y pulsamos el botón derecho del ratón sobre la cuenta Director.



c) Pulsamos sobre mover y aparecerá la ventana de selección del destino de la cuenta, en este caso la unidad organizativa de Académicos



d) Seleccionarla y dar **OK**, y en ese momento de hace el movimiento de la cuenta al destino especificado.

WINDOWS 2003 SERVER ®

Tema 4

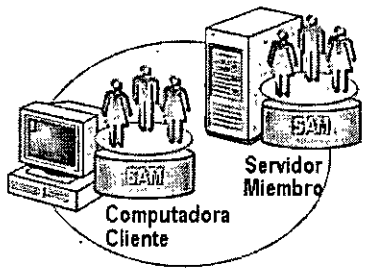
Administración de grupos

- Crear grupos
- Administrar a los miembros del grupo
- Estrategias para utilizar grupos
- Modificar grupos
- Utilizar grupos predeterminados
- prácticos para administrar grupos

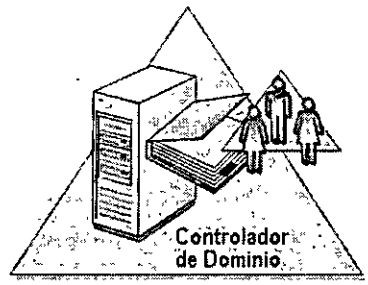
FLORES ALVARES LUIS ARMANDO
GUERRERO MARTINEZ EDSON ARMANDO

Crear grupos.

Los grupos son también objetos del directorio, a estos se les asignan automáticamente identificadores de seguridad, se utilizan para reunir las cuentas de usuario, las cuentas de equipo y otras cuentas de grupo en unidades administrables. Los grupos funcionan de distinta manera en un dominio y en un grupo de trabajo.



Grupo de Trabajo



Dominio

Grupos en un Grupo de Trabajo:

-Son creados en computadoras que no son controladores de dominio.

-Son utilizados para otorgar permisos a los recursos y otorgar derechos para tareas de sistema solo en la computadora en la cual se crea el grupo.

-Se localizan en el **SAM** (Security Account Management).

Grupos en un Dominio:

-Se crean solo en los controladores de dominio.

-Son utilizados para otorgar permisos a los recursos y otorgar derechos para tareas de sistema en cualquier computadora del dominio.

-Residen en el servicio del **Active Directory**

Tipos de Grupos:

En el **Active Directory** de Windows Server 2003 ® hay dos tipos de grupos:

-De distribución.- en este tipo no es posible habilitar la seguridad, ya que no aparecen en las listas de control de acceso discrecional. Sólo se pueden utilizar con aplicaciones de correo electrónico (como Microsoft Exchange) para enviar correo elctronico a los grupos de usuarios y no para asignar derechos ni permisos.

-De seguridad.- Se muestra en las listas de control de acceso discrecional (DACL), que constituye el lugar donde están definidos los premisos sobre los recursos y los objetos. Los grupos de seguridad se usan para asignar derechos y permisos, los grupos de seguridad suponen un modo eficaz de asignar el acceso a los recursos de su red.

Los grupos también se pueden clasificar en función de su ámbito de aplicación que identifica el alcance de aplicación del grupo:

-Grupos locales.- Solo se pueden crear en equipos que no tienen instalado el **Active Directory.** Pueden tener como miembros a cuentas locales del equipo en el que se crean, si el equipo forma parte de un dominio, pueden tener también cuentas y grupos del propio dominio y de los dominios de confianza, y se pueden utilizar para conceder permisos en el equipo en el que se crea el grupo

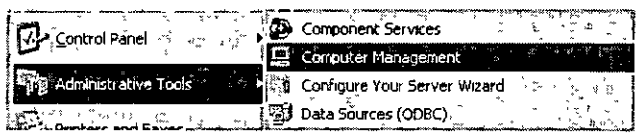
-De ámbito local de dominio.- Solo se pueden crear en servidores que tenga instalado el **Active Directory.** Pueden tener como miembros a grupos universales, grupos globales, grupos locales de su propio dominio y cuentas de cualquier dominio, y sólo se pueden utilizar para conceder permisos en el dominio que contiene el grupo.

-De ámbito global.- Solo se pueden crear en servidores que tenga instalado el **Active Directory.** Pueden tener como miembros a grupos globales y cuentas únicamente del dominio en el que se ha definido el grupo, y se les puede conceder permisos en cualquier dominio.

-De ámbito universal.- Solo se pueden crear en servidores que tenga instalado el **Active Directory.** Pueden tener como miembros a otros grupos universales, grupos globales y cuentas de cualquier dominio y se le pueden conceder permisos en cualquier dominio.

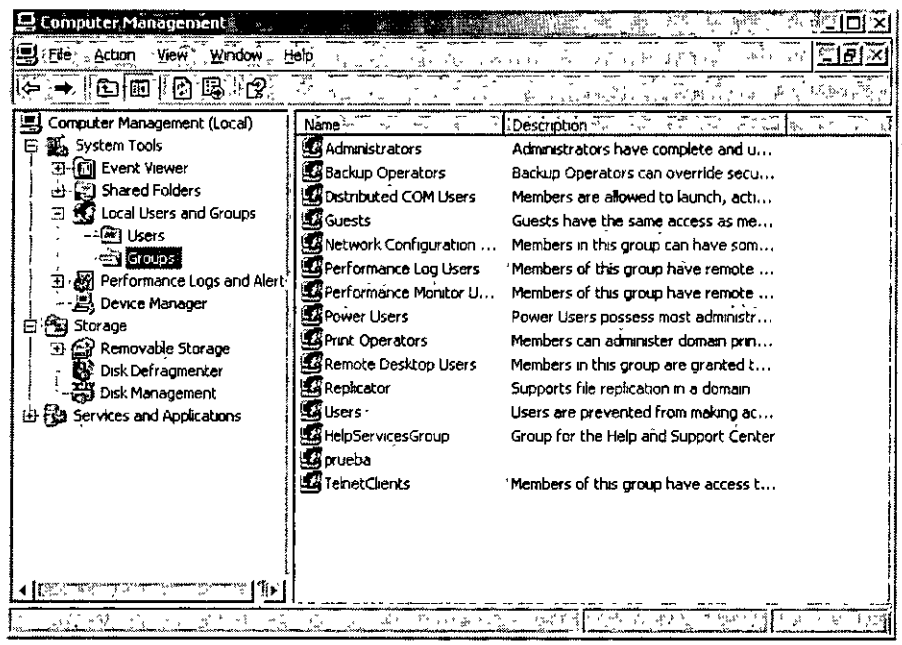
Creación de grupos locales.

1. Seleccione **Computer Management** de **Administrative Tools** del menú **Start.**

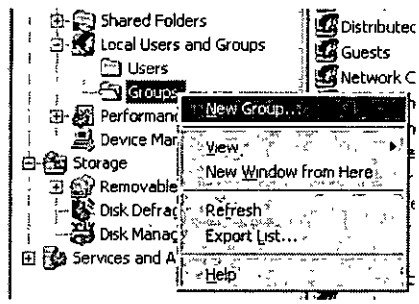


2. Pulse el botón izquierdo del ratón sobre el signo "+" que hay a la izquierda de **Local Users and Goups**, se encuentra en el panel izquierdo, y se desplegara su contenido, **Users** y **Groups.**

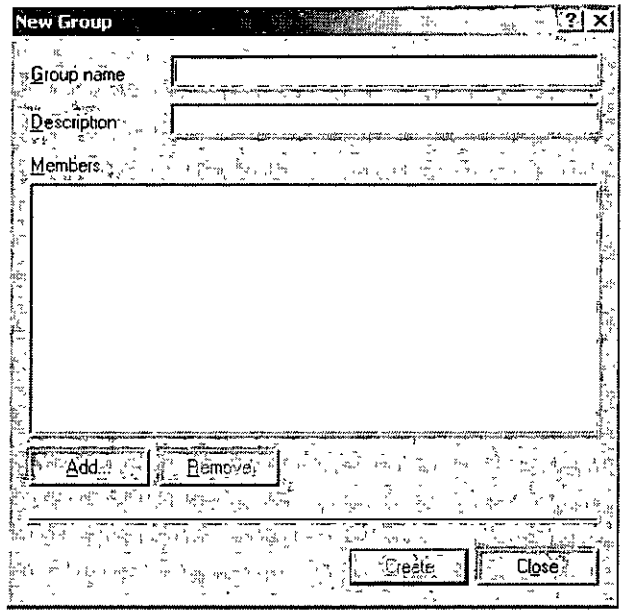
3. Pulse el botón izquierdo del ratón sobre **Groups**, en el panel derecho se mostraran los grupos que hay dados de alta en el equipo.



4. Pulse el botón derecho del ratón sobre **Groups** para que muestre su menú contextual, seleccione **New Group.**



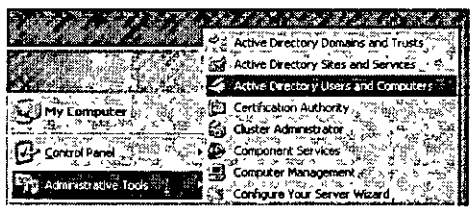
5. Se mostrará la siguiente pantalla en donde se deberá indicar el nombre que se le desea dar al grupo y una breve descripción.

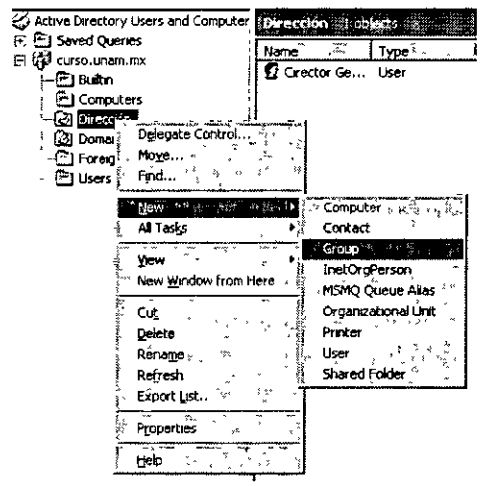


6. Se puede dar clic en el botón **Add** para agregar los usuarios, identidades o grupos que se deseen. Una vez que se haya finalizado esta operación dar clic en **Create.**

Creación de grupos globales, universales y locales de dominio.

1. Seleccione **Active Directory Users and Computers** de **Administrative Tools** del menú **Start**.

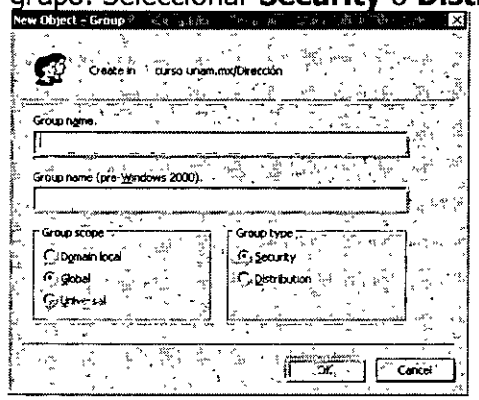




2. Dar clic con el botón derecho en el directorio en el cual se quiere crear el grupo, apuntar a **New**, y después dar clic en **Group.**

3. Aparecerá una ventana que nos permitirá crear el grupo y en donde tenemos que ingresar los siguientes valores:

- ➔ **Group name:** El nombre del grupo. El nombre debe ser único en el dominio donde se crea el grupo.
- ➔ **Group name (pre-Windows 2000):** El nombre utilizado para soportar clientes y servidores de versiones anteriores de Windows 2003 ®.
- ➔ **Group scope:** Es el alcance del grupo. Seleccionar Domain Local, Global o Universal.
- ➔ **Group type:** El tipo de grupo. Seleccionar **Security** o **Distribution.**



4. Dar clic en OK. Con esto se creara un grupo que no tiene a nadie como miembro, para indicar miembros a grupos pasar a administrar grupos.

Administrar a los miembros del grupo.

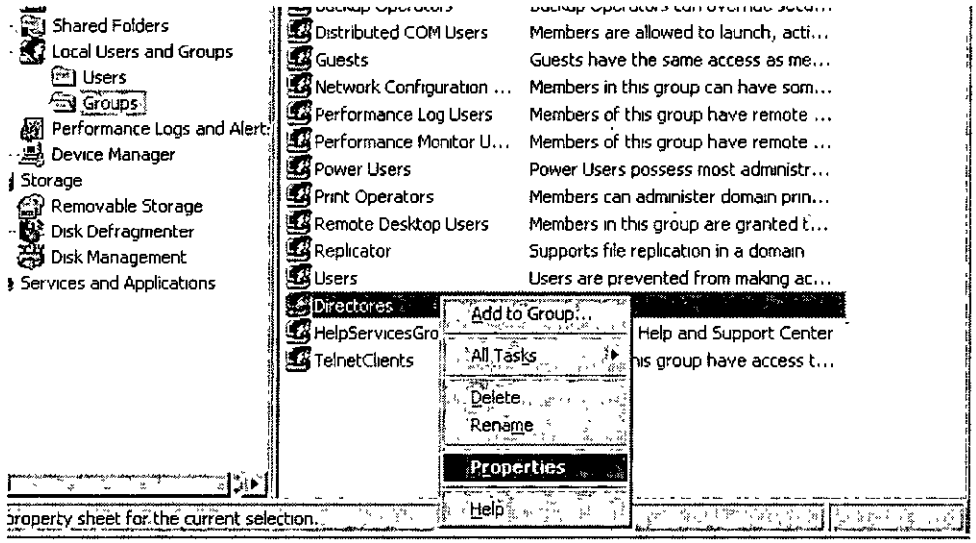
Administrar a los miembros de grupos locales.

1. Seleccione **Computer Management** de **Administrative Tools** del menú **Start.**

2. Pulse el botón izquierdo del ratón sobre el signo "+" que hay a la izquierda de **Local Users and Groups**, se encuentra en el panel izquierdo, y se desplegara su contenido**, Users** y **Groups.**

3. Pulse el botón derecho del ratón sobre **Groups**, en el panel derecho se mostraran los grupos que hay dados de alta en el equipo.

4. Pulse el botón derecho del ratón sobre el grupo que se desea modificar para que muestre su menú contextual, seleccione **Properties.**

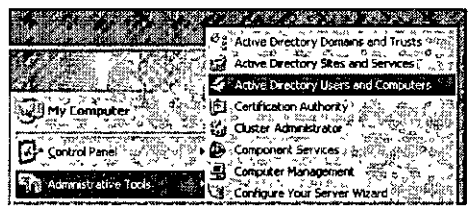


5. Aparecerá una ventana con la ficha General en donde se encuentran los siguientes apartados:

-Name: Muestra el nombre del grupo, el cual puede ser cambiado.
-Description: Muestra una breve descripción del grupo.
-Miembros: Muestra los usuarios, identidades especiales o grupos que son miembros de este grupo. Si marca en **Add,** pulse en **Advanced,** pulse en **Find Now**, seleccione los usuarios, identidades especiales o grupos que desee, pulse en OK y vuelva a pulsar en OK, puede añadir más miembros al grupo. Si se sitúa sobre un miembro de la lista y marca en **Remove**, lo eliminará.

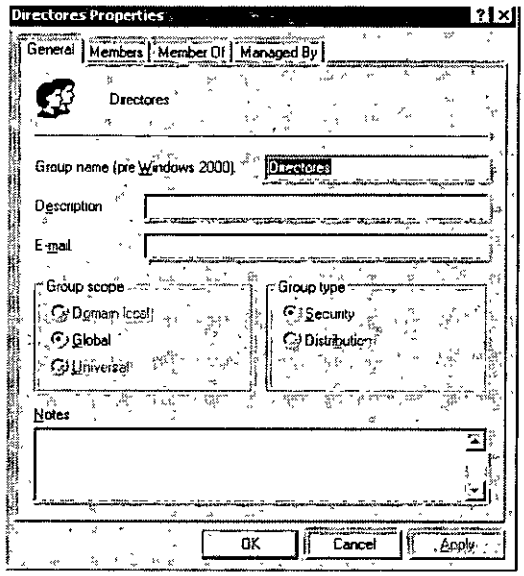
Administrar a miembros de grupos globales, universales y locales de dominio

1. Seleccione **Active Directory Users and Computers** de **Administrative Tools** del menú **Start.**



2. Pulse el botón izquierdo del ratón sobre la carpeta en la cual se encuentre el grupo al que desea añadir miembros y, en el panel derecho, le mostrará los usuarios o grupos que hay dados de alta en esa carpeta del **Active Directory.**

3. Sitúese sobre el grupo que desea modificar, pulse el botón derecho del ratón para que muestre su menú contextual, seleccionar **Propierties** y se mostrará la siguiente pantalla:

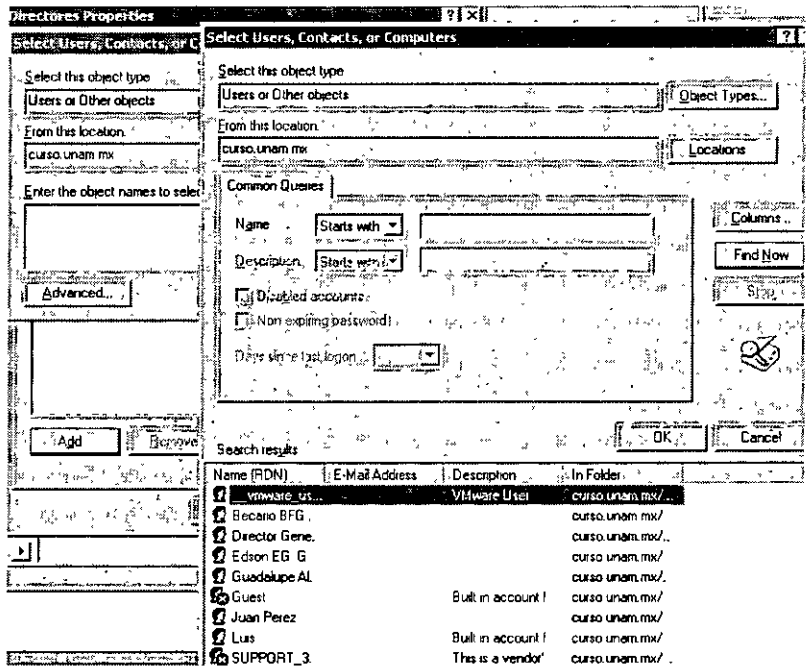


4. Seleccionar la ficha **Members,** en esta ficha aparecerán los nombres de los miembros de este grupo. Para agregar un miembro dar clic en el botón **Add,** después pulsar el botón **Advanced,** posteriormente pulsar **Find Now,** seleccionar los usuarios que desea agregar como miembros de este grupo, dar clic en OK, y otra vez en OK. Podrá añadir más usuarios a la lista y, si se sitúa sobre un grupo de la lista y marca **Remove**, lo eliminara

5. Si pulsa la ficha **Member Of,** verá una pantalla que muestra los grupos de dominio local y los grupos universales a los que pertenece el grupo seleccionado. Si marca en **Add,** pulsa en **Advanced,** pulsa en **Find Now,** selecciona los grupos que desea, pulsa en *OK* y vuelve a pulsar en *OK,* podrá añadir más grupos a la lista y, , si se sitúa sobre un grupo de la lista y marca **Remove,** lo eliminara

En la ventana **Select User, Contacts, Computers, or Group** se encuentran:

-Object Types. Te permite seleccionar entre varios tipos de objetos a buscar.
-Locations: El Dominio u OU donde se buscaran los objetos.
-Check Names: Verifica la correcta escritura de los nombres de usuario.
-Advanced: Te permite realizar la búsqueda de algún objeto.

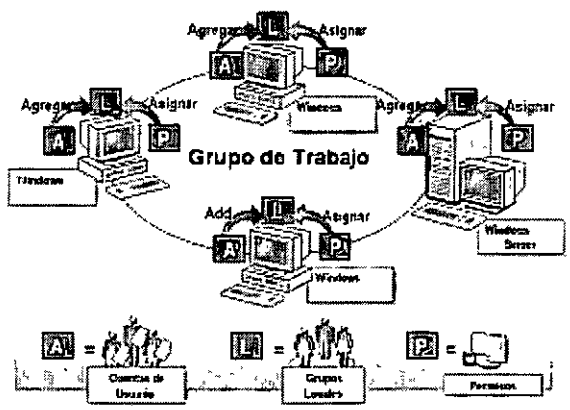


Estrategias para utilizar grupos

Estrategia para Utilizar Grupos Locales en un Grupo de Trabajo

En un ambiente de grupo de trabajo, la estrategia a utilizar para otorgar permisos u otorgar derechos es simple. Primeramente, solo se pueden utilizar grupos locales en la computadora local. Cualquier usuario que quiera obtener acceso a un recurso compartido o realizar una tarea de sistema en una computadora debe tener una cuenta de usuario en la computadora.

Si múltiples usuarios en una computadora requieren acceso al mismo recurso o necesitan realizar la misma tarea de sistema, se puede utilizar un grupo local para otorgar los permisos o derechos y después agregar las cuentas de usuario apropiadas como miembros.



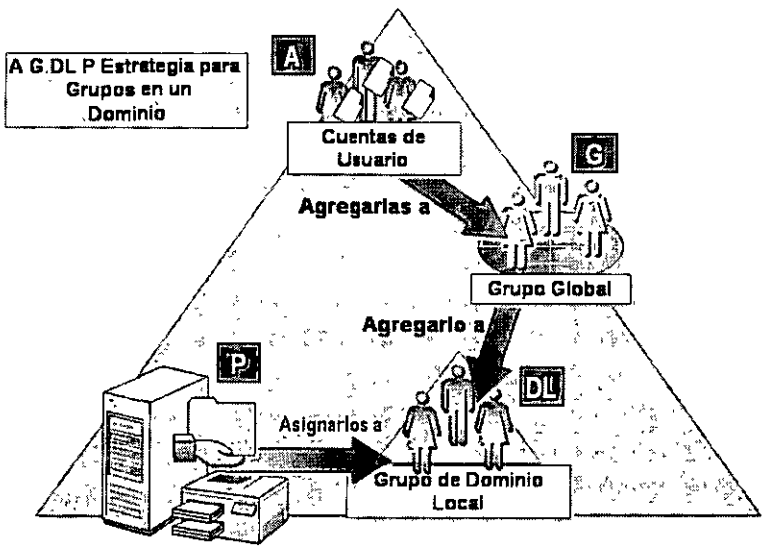
Este método es conocido como estrategia **ALP**:

-Agregar cuentas de usuario (A) a un grupo local (L) en la computadora en la cual los recursos de red residen o en la cual serán realizadas las tareas de sistema.

-Otorgar permisos (P) u otorgar derechos al grupo local en la computadora en la cual residen los recursos de red o en la cual serán realizadas las tareas de sistema.

Grupos en un solo dominio

Cuando se utilizan grupos en un solo dominio, se puede utilizar la estrategia A G DL P. La estrategia A G DL P es: colocar las cuentas de usuario (A) en grupos globales (G), colocar los grupos globales en grupos de dominio local (DL) y después otorgar permisos (P) al grupo de dominio local.



A = Users Accounts
G = Global Groups
DL= Domain Local Groups
P = Permissions

Esto quiere decir qué:

Agrupamos a los usuarios en un Grupo Global, y éstos se agrupan en un grupo local de dominio, ya sea uno de los existentes o cualquier otro que hayamos creado nosotros, toda vez que tenemos el anidamiento aplicaríamos los permisos a los recursos, archivos, impresoras, etc... al Grupo Local de Dominio, y no a los grupos globales ni a los usuarios.

Cuando se crean grupos, se debería seguir la siguiente estrategia:

1. Identificar los usuarios con responsabilidades comunes y agregar las cuentas de usuario a un grupo Global. Por ejemplo, en el departamento de ventas, agregar las cuentas de usuario para todos los empleados de ventas que utilicen los mismos recursos a un grupo Global llamado Ventas.

2. Determinar si se puede utilizar un grupo de Dominio Local Incorporado, o si necesitas crear uno para proporcionar a los usuarios acceso a los recursos de dominio. Por ejemplo, si se quiere que los usuarios sean capaces de imprimir en una impresora de color compartida en el dominio, se puede crear un grupo de Dominio Local llamado Usuarios Impresora Color.

3. Hacer a todos los grupos Globales que comparten las mismas necesidades de acceso a los recursos miembros del grupo de dominio local apropiado. Por ejemplo, agregar los grupos Globales apropiados, incluyendo Ventas, al grupo de Dominio Local Usuarios Impresora Color.

4. Otorgar los permisos requeridos al grupo de Dominio Local en el controlador de dominio. Se pueden otorgar los permisos al recurso. Por ejemplo, se pueden otorgar los permisos necesarios para utilizar impresoras de color para el grupo de Dominio Local Usuarios Impresora Color.

Anidamiento y las diversas estrategias posibles en múltiples dominios.

¿Qué es el anidamiento de grupos?

Al utilizar el anidamiento de grupos lo que se hace es hacer a un grupo miembro de otro. Las opciones dependerán del nivel de funcionalidad del dominio establecido.

Un grupo Universal puede contener cuentas de usuario, cuentas de equipo, otros grupos universales y globales de cualquier dominio.

Un grupo global puede contener cuentas de usuario, cuentas de equipo, grupos universales y globales del mismo dominio del grupo global.

Un grupo de dominio local puede contener cuentas de usuario, grupos universales y globales de cualquier dominio. Además pueden contener otros grupos de dominio local del mismo dominio.

Consejo: Minimiza el anidamiento, un sólo nivel de anidamiento es el más efectivo método, porque el seguimiento de los permisos se complica con múltiples niveles.

Estrategias de grupo

Si queremos utilizar grupos de forma efectiva necesitaremos pensar en unas estrategias para aplicarlas a los diferentes ámbitos de grupo. La elección de éstas depende del entorno de la Red Windows de tu empresa. En un dominio simple, la práctica más común es utilizar grupos globales y de dominio local para asignar permisos a los recursos de la red. En entornos de múltiples dominios, se pueden añadir grupos globales y universales en la estrategia.

Con **A G P**, emplazas cuentas de usuarios(A) en grupos globales(G) y les asignas permisos(P) a los grupos globales. La limitación de ésta es que se complica su administración en múltiples dominios. Si los grupos globales de varios dominios requieren los mismos permisos, entonces debes asignarlos a cada grupo global individualmente.

Esta estrategia (**A G P**) se puede utilizar en bosques de un sólo dominio y pocos usuarios y al que no se añadirán otros dominios.

- Tiene las ventajas de que los grupos no necesitan anidamiento y por tanto la solución de problemas es más fácil, y las cuentas pertenecen a un ámbito de grupo sólo.

- Las desventajas son que cada vez que un usuario se autentica en un recurso, el servidor debe comprobar el grupo global al que pertenece para determinar si el usuario todavía es miembro del grupo. Y el funcionamiento se degrada ya que un grupo global no se guarda en caché.

Con **A DL P**, emplazamos cuentas de usuario(A) en grupos de dominio local(DL) al que damos permisos(P). Una limitación de ésta estrategia es que no podemos asignar permisos a recursos fuera del dominio. Por lo tanto, esto reduce la flexibilidad según la red va creciendo.

Podemos utilizarla en un bosque donde se cumple lo siguiente:
- Sólo hay un dominio y pocos usuarios.
- Nunca añadirás otros dominios al bosque.
- No hay servidores miembros con Windows NT en el dominio.

Tiene las ventajas de que las cuentas pertenecen a un ámbito de grupo sólo y los grupos no están anidados facilitando la resolución de problemas.

En cambio, el funcionamiento se degrada, porque cada grupo de dominio local tiene demasiados miembros que deben ser autenticados.

A G DL P, aquí emplazamos cuentas de usuario(A) en grupos globales(G), y a éstos en grupos de dominio local(DL) a los que damos permisos(P). Esta estrategia quizás ofrece mayor flexibilidad para el crecimiento de la red y reduzca el número de veces en que necesitamos configurar permisos.

Podemos utilizarla en un bosque consistente en uno o más dominios y al que añadiremos otros en el futuro.

Cuenta con las ventajas de que los dominios son flexibles y los propietarios de los recursos requieren menor acceso a **Active Directory** para asegurar la flexibilidad de sus recursos.

Como desventaja diremos que es una estructura escalonada más compleja en su inicio, pero más fácil de manejar al pasar el tiempo.

A G U DL P, emplazamos cuentas de usuarios(A), en grupos globales(G), estos en grupos Universales(U), que a su vez emplazamos en grupos de dominio local(DL), a los que les asignamos permisos(P).

Dicha estrategia se utilizaría en un bosque con más de un dominio donde los administradores necesitan administración centralizada para muchos grupos globales.

- Sus ventajas serían una flexibilidad a lo largo del bosque y la administración estaría centralizada.
(Los grupos de dominio local no deberían usarse para asignar permisos a objetos de AD en un bosque con más de un dominio.).

Como desventajas nos encontramos con:

- Que los miembros de los grupos universales se almacenan en el catálogo global. (El catálogo global es un DC que almacena una copia de TODOS los objetos del AD en un bosque. El catálogo global almacena copia completa de todos los objetos de AD de su propio dominio y una copia parcial de todos los objetos de los otros dominios del bosque).
- Puede ser necesario añadir más servidores catálogo global.

- Se aumenta la latencia de la replicación de catálogo global, referido al tiempo que se tarda en replicar cada servidor catálogo global en el bosque.

Hay una desventaja al usar grupos Universales, sólo si estos tienen muchos miembros dinámicos con un tráfico alto de replicación de catálogo global, por los cambios en sus miembros, en un bosque multidominios. Con **G U DL P**, esto es menor porque los miembros de los grupos universales son relativamente estáticos (esto es, contiene grupos globales, no usuarios individuales).

A G L P, esta estrategia está limitada a los recursos del equipo local.

Puede utilizarse el mismo grupo global en múltiples equipos locales.

Esta estrategia podría usarse si el dominio cumple ciertas características:
- Se ha actualizado desde Windows NT ® a Windows Server 2003 ®.
- Contiene un sólo dominio.
- Tiene pocos usuarios.
- No se añadirán nunca otros dominios.
- Para mantener estrategia de grupos de Windows NT ®.
- Para mantener centralizada la administración de usuarios y descentralizada la de recursos.

Es recomendable en todo caso si hay servidores miembros que ejecutan Windows NT server dentro de un AD de Windows Server 2003 ®.

Las ventajas vienen determinadas por la estrategia de mantener los grupos de NT y los propietarios de los recursos son miembros de cada grupo que necesita acceso.

Las desventajas son que AD no mantiene ningún control, se crean grupos repetidos en los servidores miembro y no puede activarse una administración centralizada.

Modificar grupos.

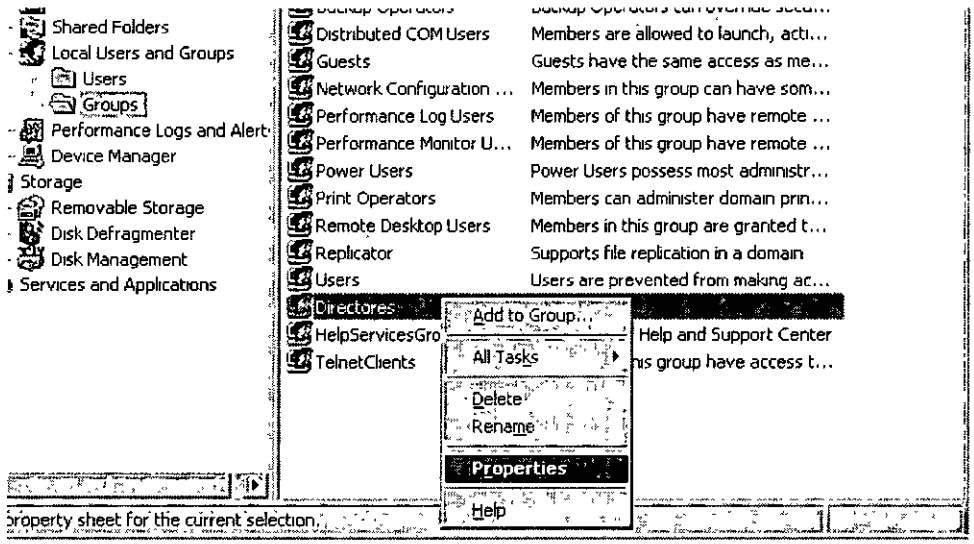
Modificar grupos locales.

1. Seleccione **Computer Management** de **Administrative Tools** del menú **Start.**

2. Pulse el botón izquierdo del ratón sobre el signo "+" que hay a la izquierda de **Local Users and Groups,** se encuentra en el panel izquierdo, y se desplegara su contenido, **Users** y **Groups.**

3. Pulse el botón derecho del ratón sobre **Groups**, en el panel derecho se mostraran los grupos que hay dados de alta en el equipo.

4. Pulse el botón derecho del ratón sobre el grupo que se desea modificar para que muestre su menú contextual, seleccione **Properties.**



5. Aparecer una ventana con la ficha General en donde se podrá modificar el nombre del grupo, la descripción y los miembros.

Cambiar nombre de grupo local

1. Seleccione **Computer Management** de **Administrative Tools** del menú **Start.**

2. Pulse el botón izquierdo del ratón sobre el signo "+" que hay a la izquierda de **Local Users and Groups**, se encuentra en el panel izquierdo, y se desplegara su contenido, **Users** y **Groups.**

3. Pulse el botón derecho del ratón sobre **Groups,** en el panel derecho se mostraran los grupos que hay dados de alta en el equipo.

4. Pulse el botón derecho del ratón sobre el grupo al que le se desea cambiar el nombre para que muestre su menú contextual, seleccione **Rename.** Teclee el nuevo nombre y de enter.

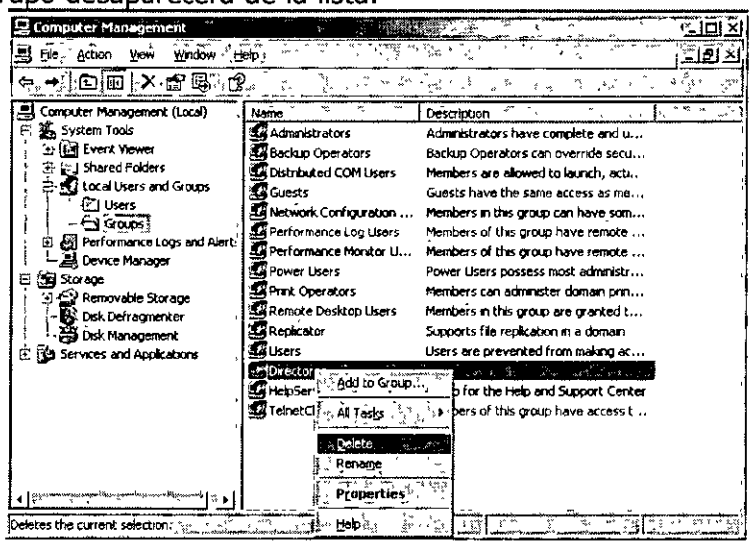
Eliminar grupos locales

5. Seleccione **Computer Management** de **Administrative Tools** del menú **Start.**

6. Pulse el botón izquierdo del ratón sobre el signo "+" que hay a la izquierda de **Local Users and Goups,** se encuentra en el panel izquierdo, y se desplegara su contenido, **Users** y **Groups.**

7. Pulse el botón derecho del ratón sobre **Groups,** en el panel derecho se mostrarán los grupos que hay dados de alta en el equipo.

8. Pulse el botón derecho del ratón sobre el grupo que se desea eliminar para que muestre su menú contextual, seleccione **Delete.** Confirme que desea realizar la acción y el grupo desaparecerá de la lista.

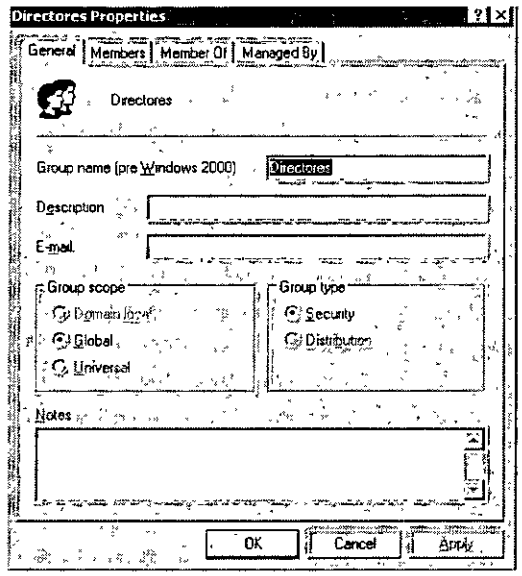


Modificar grupos globales, universales y locales de dominio.

1. Seleccione **Active Directory Users and Computers** de **Administrative Tools** del menú **Start.**

2. Pulse el botón izquierdo del ratón sobre la carpeta en la cual se encuentre el grupo al que desea modificar, en el panel derecho, le mostrará los usuarios o grupos que hay dados de alta en esa carpeta den el **Active Directory.**

3. Sitúese sobre el grupo que desea modificar, pulse el botón derecho del ratón para que muestre su menú contextual, seleccionar **Propierties** y se mostrará la siguiente pantalla:



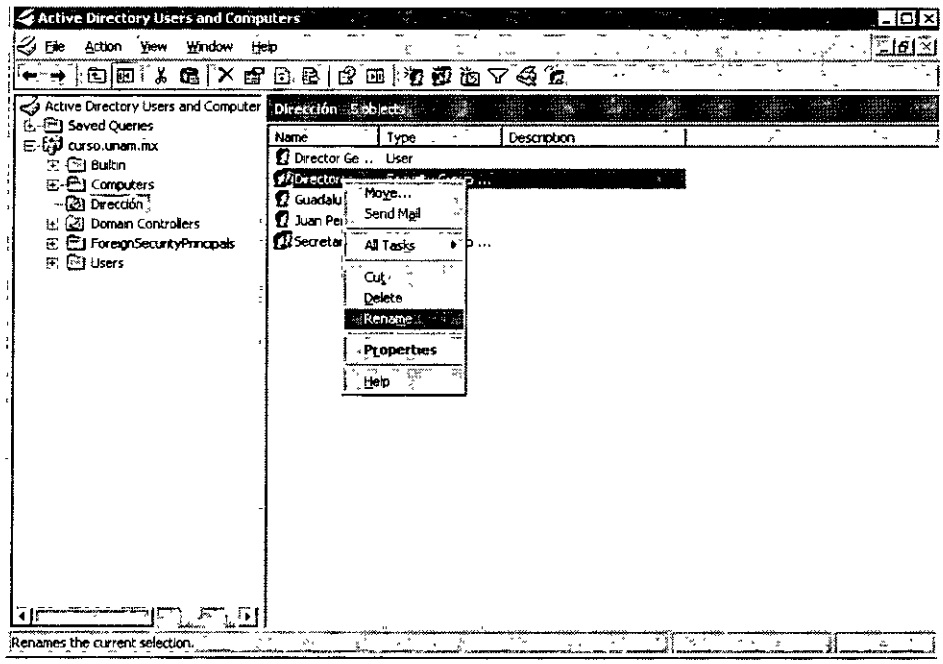
En esta ventana podremos cambiar el nombre, la descripción, los miembros que contiene este grupo, y también podemos cambiar a que miembros pertenece, así como por quien está administrado.

Cambiar nombre a grupos globales, universales y locales de dominio

1. Seleccione **Active Directory Users and Computers** de **Administrative Tools** del menú **Start.**

2. Pulse el botón izquierdo del ratón sobre la carpeta en la cual se encuentre el grupo al que desea cambiarle el nombre y, en el panel derecho, le mostrará los usuarios o grupos que hay dados de alta en esa carpeta de el **Active Directory.**

3. Sitúese sobre el grupo que desea modificar, pulse el botón derecho del ratón para que muestre su menú contextual, seleccionar **Rename.** Teclee el nuevo nombre y de enter.



Eliminar grupos globales, universales y locales de dominio

1. Seleccione **Active Directory Users and Computers** de **Administrative Tools** del menú **Start.**

2. Pulse el botón izquierdo del ratón sobre la carpeta en la cual se encuentre el grupo al que desea eliminar y, en el panel derecho, le mostrará los usuarios o grupos que hay dados de alta en esa carpeta de el **Active Directory.**

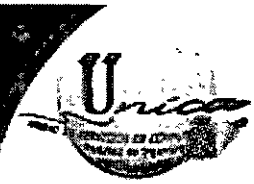
3. Sitúese sobre el grupo que desea modificar, pulse el botón derecho del ratón para que muestre su menú contextual, seleccionar **Delete.** Teclee el nuevo nombre y de enter.

Utilizar grupos predeterminados

Grupos Locales Incorporados (Built-in)

Windows 2003 automáticamente crea grupos cuando se instala Windows 2003 Server ® en una computadora o Windows 2000 ® en un servidor miembro. Estos grupos incorporados tienen un conjunto de derechos predeterminados. Los derechos determinan las tareas de sistema que un usuario puede realizar. No es posible eliminar los grupos incorporados.

Los grupos incorporados en computadoras ejecutando Windows 2003 Server ® y servidores miembros son:



- **Grupos Locales Incorporados.** Estos grupos dan a sus miembros los derechos para realizar tareas de sistema como respaldar y restaurar archivos, cambiar la hora del sistema y administrar recursos de sistema. Los grupos incorporados están en todas las computadoras ejecutando Windows 2003 Server ®. Residen en el directorio **Groups** en **Local Users and Groups** en **Computer Management.**

- **Identidades Especiales.** Estos grupos también conocidos como grupos especiales, organizan automáticamente a los usuarios para utilizar el sistema. Los administradores no pueden modificar la membresía a estos grupos. Por lo tanto, los usuarios son miembros de forma predeterminada o llegan a ser miembros durante las actividades. Los grupos especiales están en todas las computadoras ejecutando Windows 2003 Server ®. Por ejemplo, cuando un usuario inicia sesión en una computadora y obtiene acceso a los recursos de la computadora, a través de la actividad de inicio de sesión, el usuario llega a ser un miembro del grupo especial Interactive.

Grupos Incorporados y Predefinidos en un Dominio

Al igual que las computadoras cliente y los servidores miembros, los controladores de dominio tienen de forma predeterminada grupos incorporados. Además de los grupos incorporados, los controladores de dominio tienen también de forma predeterminada grupos predefinidos. Cuando una computadora llega a ser un controlador de dominio, Windows 2003 Server ® automáticamente crea estos grupos en **Active Directory Users and Computers.** Al igual que los grupos locales incorporados, estos grupos tienen derechos predeterminados, los cuales determinan las tareas de sistema que los miembros de un grupo incorporado o predefinido pueden realizar.

Los grupos predefinidos con alcance global están localizados en el directorio **User**. Los grupos incorporados con alcance de dominio local están localizados en el directorio **Builtin.** Los grupos de dominio predeterminados en Windows 2003 Server ® incluyen:

- **Grupos Incorporados de Dominio Local.** Estos grupos proporcionan usuarios con derechos y permisos predefinidos para realizar tareas en los controladores de dominio y en **Active Directory.** Los grupos incorporados de dominio local se encuentran solamente en los controladores de dominio. No es posible eliminar estos grupos.

- **Identidades Especiales.** Estos grupos, también conocidos como grupos especiales, organizan automáticamente a los usuarios para el uso del sistema. Los administradores no asignan usuarios a ellos. De tal forma, los usuarios los usuario son miembros de forma predeterminada o llegan a ser miembros durante la actividad de red. Los grupos de sistema están en todas las computadoras ejecutando Windows 2000 ®.

Por ejemplo, cuando los usuarios se conectan al directorio compartido en una computadora remota, llegan a ser miembros del grupo **Network System.** Los grupos especiales no son visibles en **Active Directory Users and Computers.**

- **Grupos Globales Predefinidos.** Estos grupos dan a los administradores una forma fácil de controlar todos los usuarios en un dominio. Los grupos globales predefinidos se encuentran solo en los controladores de dominio. Estos grupos residen en el directorio **Users** de **Active Directory.**

Grupos predeterminados en un servidor miembro

Algunos de estos grupos son Administrators, Guests, Performance Log Users, Performance Monitor Users, Power Users, Print Operators Users, Network Configuration Operators, Remote Desktop Users, Replicator, HelpServicesGroup, Terminal Server Users, etc.

Grupos predeterminados en Active Directory.

Algunos de estos grupos son: Account Operators, Incoming Forest Trust Builders, Pre-Windows 2000 Compatible Access, Server Operators, Domain Controllers, Domain Guests, Domain Users, Domain Computers, Domain Admins, Enterprise Admins, Group Policy Creator Owners, Schema Admins, DnsAdmins, DnsUpdateProxy, Cert Publishers, RAS and IAS Servers.

Consejos prácticos para administrar grupos

Lineamientos para la Creación de Grupos de Dominios.

Cuando se crean grupos para utilizarse en un dominio, se debería considerar los siguientes lineamientos:

- Determinar el alcance del grupo requerido en base a la forma en que se quiere utilizar el grupo. Por ejemplo, utilizar grupos globales para agrupar cuentas de usuario.

- Determinar si se tienen los permisos necesarios para crear un grupo en el dominio apropiado:

  (1) De forma predeterminada, los miembros de los grupos **Administrators** y **Account Operators** en un dominio tienen los permisos necesarios para crear grupos.

  (2) Un administrador puede dar a un usuario los permisos para crear grupos en el dominio.

- Determinar el nombre del grupo. Hacer el nombre intuitivo para que refleje el propósito para el cual fue creado el grupo. Esto es útil especialmente si los de otros dominios buscan estos grupos en **Active Directory.**

Mejores prácticas

La siguiente lista proporciona las mejores prácticas para la implementación de grupos:

- Crear grupos en base a las funciones de trabajo. Cuando se crea un grupo en base a una función de trabajo y otras personas toman este trabajo, solo es necesario cambiar la membresía de grupo. No se necesitan cambiar todos los permisos que son otorgados a la cuenta de usuario individual. Debido a esto, es algunas veces ventajoso crear un grupo que tenga solamente un miembro.

- Utilizar grupos locales solo en computadoras que no pertenecen a un dominio, debido a que no se puede administrar de forma centralizada grupos locales.

- Cuando existan múltiples grupos de los cuales se puede echar mano, siempre se debe agregar cuentas de usuario al grupo que sea el más restrictivo, de tal forma que solo se permitan los derechos y permisos apropiados para permitir a los usuarios realizar cualquier tarea requerida.

- Si existe un grupo incorporado que permita a los usuarios realizar una tarea, utilice este grupo en lugar de crear un nuevo grupo. Solo se deben crear grupos cuando no existan grupos incorporados que proporcionen los derechos y permisos requeridos.

WINDOWS 2003 SERVER ®

Tema 5

Administración de acceso a los recursos

- Introducción a la administración del acceso a los recursos
- Administrar acceso a carpetas compartidas
- Administrar acceso a archivos y carpetas utilizando permisos NTFS
- Determinar permisos eficaces
- Administrar acceso a archivos compartidos utilizando la Caché sin conexión implementar la impresión.

FLORES ALVAREZ LUIS ARMANDO
GUERRERO MARTÍNEZ EDSON ARMANDO

+

Introducción a la administración del acceso a los recursos

En este apartado se va a tratar la configuración y el uso de la red Microsoft ® bajo el sistema operativo Windows 2003 Server ®. Cuando un sistema Windows 2003 Server ® participa en una red (grupo de trabajo o dominio), puede compartir sus recursos con el resto de ordenadores.

Al compartir una carpeta con la red, permitimos el acceso a la carpeta y a los ficheros que contiene. Pero también podemos controlar qué usuarios acceden, a qué recursos y con qué permisos.

La manera clásica de compartir permite controlar quién accede a cada recurso (contraponiéndose a permitir el acceso a "cualquiera" de la red), y con qué permisos: por ejemplo, sólo lectura, o bien actualización.

El compartir de manera clásica conlleva tres cambios fundamentales:

* Podemos especificar permisos básicos en recursos compartidos -simple file sharing- (esto coloca permisos solo para el grupo "Everyone").

* Si la carpeta compartida está en un volumen NTFS, podemos crear ACL's (listas de control de acceso) en cada objeto del recurso compartido ("simple file sharing" pone permisos en NTFS sólo para el grupo "Everyone", y oculta la posibilidad de ver o modificar ACL's).

* Los usuarios que se conectan a nuestra máquina bajo la red, no serán autenticados como "Invitados". Si el nombre del usuario de la red y una password distinto de blancos coincide con el nombre y password de una cuenta dada de alta en nuestra máquina, Windows ® autentifica el usuario con la cuenta local. Si el usuario de red, nombre y password no coincide con una cuenta local, entonces Windows ® lo autenticará como invitado (si este estuviese configurado para admitir conexiones por red).

Es muy importante este último párrafo ya que explica la manera de autenticar al usuario que posee Windows 2003 Server ® cuando está funcionando como grupo de trabajo. La autenticación en Dominio es totalmente diferente.

Cualquier sistema Windows 2003 Server ® puede compartir carpetas, no importando si es un servidor o si es una estación de trabajo. Para poder compartir una carpeta basta con desplegar su menú contextual desde una ventana o desde el explorador de archivos y seleccionar Compartir... En la ventana asociada a esta opción se determina el nombre que tendrá el recurso (que no tiene por qué coincidir con el nombre de la propia carpeta), así como qué usuarios podrán acceder al mismo. En relación con esto, existe una gran diferencia entre que el directorio resida en una partición FAT y que resida en una NTFS.
Si la carpeta reside en una partición FAT, este filtro de acceso será el único que determine a los usuarios que van a poder acceder al contenido de la carpeta, puesto que no es posible determinar permisos sobre la misma o sobre sus archivos. Es decir, el filtro sólo se establece para poder acceder al recurso. Si un usuario tiene permisos suficientes para conectarse a un recurso, tendrá acceso a todos los archivos y subcarpetas del mismo. Concretamente, el tipo de acceso sobre todos ellos será el que defina el permiso sobre el recurso (Lectura, Escritura o Control Total).

Por el contrario, si la carpeta se encuentra en una partición NTFS, ésta tendrá unos permisos establecidos (así como sus subcarpetas y archivos), no importando si está compartida o no. En este caso también es posible establecer permisos desde la ventana de Compartir..., pero sólo los usuarios que puedan *pasar* ambos filtros podrán acceder a la carpeta compartida y a su contenido.

Cuando compartimos recursos a otros usuarios en la red (especialmente en un dominio) hay que tener en cuenta no sólo los permisos del recurso y su contenido, sino también los *derechos* del ordenador que comparte el recurso. En concreto, si un usuario A ha iniciado una sesión interactiva en un ordenador Windows 2003 Server ®, y desea conectarse a un recurso de red que exporta otro Windows 2003 Server ® denominado B, además de poseer suficientes permisos (sobre el recurso, sobre la propia carpeta y sobre su contenido) tiene que tener concedido en B el derecho *Acceder* a este equipo desde la red. De lo contrario, dicho usuario ni siquiera podrá obtener la lista de los recursos que el ordenador A comparte.

Conforme avancemos en las prácticas, iremos conociendo como podemos acceder a los recursos utilizando un dominio. Mientras tanto abordaremos algunos temas importantes que usa Windows 2003 Server ® para compartir los recursos.

Permisos NTFS

Se pueden utilizar permisos NTFS para especificar que usuarios, grupos y computadoras pueden acceder a archivos y directorios. Los permisos NTFS también indican lo que los usuarios, grupos y computadoras pueden hacer con el contenido del archivo o directorio.

Permisos NTFS de Directorios

Se pueden otorgar Permisos de Directorio para controlar el acceso a directorios, archivos y subdirectorios que están contenidos dentro de estos.

A continuación se muestra una lista de los permisos NTFS estándar de directorios que se pueden otorgar y el tipo de acceso que proporciona cada uno.

Permiso NTFS de Directorio	Permite al usuario:
Read	Mostrar archivos y subdirectorios en el directorio, visualizar los atributos, propietario y permisos para directorio.
Write	Crear nuevos archivos y subdirectorios dentro del directorio, cambiar atributos de directorio, visualizar al propietario y a los permisos para los directorios.
List Folder Contents	Mostrar los nombres de archivos y subdirectorios en el directorio.
Read & Execute	Recorrer directorios, además de las acciones permitidas por Read y List Folder Contents.
Modify	Eliminar el directorio y realizar las acciones permitidas por Write y Read & Execute.
Full Control	Cambiar los permisos, tomar propiedad del archivo, eliminar subdirectorios y archivos, y realizar las acciones permitidas por todos los otros Permisos NTFS de Directorios.

Permisos NTFS de Archivos

Se pueden otorgar Permisos de Archivo para controlar el acceso a los archivos.

La tabla siguiente muestra una lista de los permisos NTFS estándar de archivos que se pueden otorgar y el tipo de acceso que proporciona cada uno de ellos a los usuarios.

Permiso NTFS de Archivo	Permite al usuario:
Read	Leer el archivo, mostrar los atributos, al propietario y los permisos para el archivo.
Write	Sobrescribir el archivo, cambiar los atributos del archivo, mostrar al propietario y los permisos del archivo.

Read & Execute	Ejecutar aplicaciones y realizar las acciones permitidas por Read.
Modif.	Modificar y eliminar el archivo, además de realizar las acciones permitidas por Write y Read & Execute.
Full Control	Cambiar permisos, tomar propiedad del archivo y realizar las acciones permitidas por todos los otros Permisos NFTS.

Formas en que se Aplican los Permisos NTFS

De forma predeterminada, cuando se otorgan permisos NTFS a los usuarios o grupos sobre un directorio, el usuario o grupos tienen acceso a los subdirectorios y archivos contenidos en el directorio. Es importante entender la forma en cómo los subdirectorios y archivos heredan los permisos NTFS de los directorios padres para poder utilizar la herencia en la propagación de permisos a archivos y directorios.

Si se otorgan permisos para un archivo o directorio a una cuenta de usuario individual o a un grupo del cual el usuario es miembro, entonces el usuario tiene múltiples permisos para el mismo recurso. Existen reglas y prioridades que están asociadas con la forma en cómo se combinan múltiples permisos NTFS. Además, también se pueden afectar los permisos cuando se copian o mueven archivos y directorios.

Múltiples Permisos NTFS

Si se otorgan permisos NTFS a una cuenta de usuario individual además del grupo al cual pertenece, entonces se otorgarán múltiples permisos al usuario. Existen reglas para la forma en cómo se combinan estos permisos para crear los permisos efectivos de usuario.

Los Permisos son Acumulativos

Los permisos efectivos de usuario para un recurso son la combinación de los permisos NTFS que se otorgan a la cuenta de usuario individual y los permisos NTFS que se otorgan al grupo o grupos a los que pertenece. Por ejemplo, si un usuario tiene permiso de *Read* para un directorio y es miembro de un grupo que tiene el permiso de *Write* en el mismo directorio, el usuario tendrá los permisos de *Read* y *Write* para éste.

Los Permisos de Archivo Sobrescriben los Permisos de Directorio

Los permisos NTFS de archivo toman prioridad sobre los permisos NTFS de directorio. Por ejemplo, un usuario con el permiso de *Change* sobre un archivo será capaz de hacer cambios a éste aún si el directorio que contiene el archivo tiene solamente el permiso de *Read*.

El Permiso Deny Sobrescribe otros Permisos

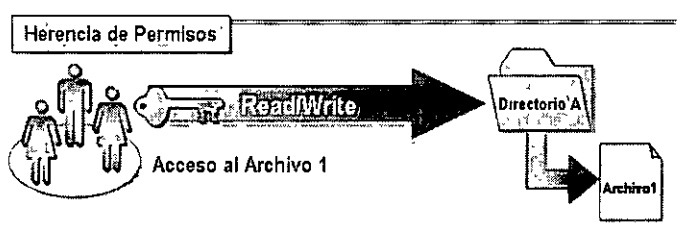
Se puede negar el acceso a archivos o directorios específicos otorgando el permiso *Deny* a la cuenta de usuario o grupo. Aún si el usuario tiene permiso de acceder al archivo o directorio como miembro de un grupo, al negar el permiso al usuario se bloqueará cualquier otro permiso que el usuario tenga. De esta forma, el permiso *Deny* es una excepción para la regla acumulativa. Se debería evitar negar permisos debido a que es mucho más fácil permitir el acceso a los usuarios y grupos que negar el acceso específicamente. Es preferible estructurar grupos y organizar recursos en directorios de tal modo que, el asignar permisos sea suficiente.

Herencia de Permisos NTFS

De forma predeterminada, los permisos que se otorgan a un directorio padre son heredados y propagados a los subdirectorios y archivos que están contenidos en directorio padre. Sin embargo, se puede evitar ésta herencia si se busca que los directorios y archivos tengan diferentes permisos que su directorio padre.

Herencia de Permisos

Cualquier permiso que se otorgue a un directorio padre también se aplicará a los subdirectorios y archivos que están contenidos dentro del mismo. Cuando se otorgan permisos NTFS para acceder a un directorio, se pueden otorgar permisos al directorio, a cualquiera de los archivos y directorios existentes, y a cualquiera de los nuevos archivos y directorios que sean creados dentro del directorio.



Prevenir la Herencia de Permisos

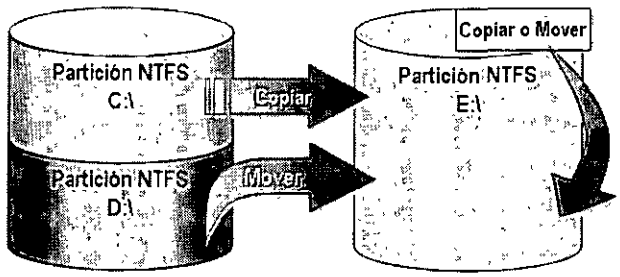
Se puede prevenir la herencia de permisos, y con ello se puede evitar que subdirectorios y archivos hereden permisos de sus directorios padres. Para prevenir la herencia de permisos, se deben remover los permisos heredados y retener solo los permisos que fueron explícitamente otorgados.

El directorio para el cual se previene la herencia de permisos de su directorio padre se convierte ahora en el nuevo directorio padre. Los subdirectorios y archivos que están contenidos dentro de este nuevo directorio padre heredan los permisos otorgados a este directorio padre.

Copiar y Mover Archivos y Directorios

Cuando se copia o se mueve un archivo o directorio, los permisos pueden cambiar dependiendo a dónde se mueve el archivo o directorio.

Es importante entender los cambios que experimentan los permisos cuando son copiados o movidos.



- **Todas las Copias Heredan los Permisos**
- **Solo Moviendo en la Misma Partición Retienen sus Permisos**

Administrar acceso a carpetas compartidas

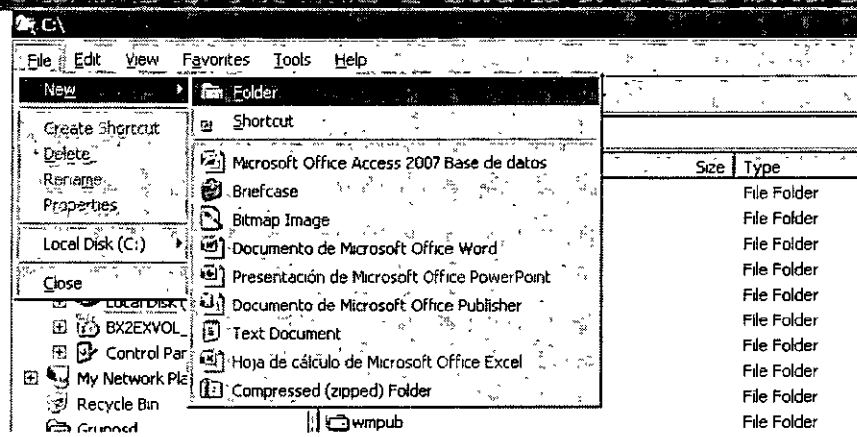
Cuando se instaló Windows 2003 Server ® con el Active Directory, se configuraron dos directorios como compartidos. Uno de ellos es \Windows\sysvol\sysvol (con el nombre compartido SYSVOL) en donde se encuentra una carpeta con el nombre del dominio el cual contiene dos subdirectorios: Policies para las directivas de grupo y Scripts para los archivos de comandos de inicio de sesión, éste subdirectorio está compartido con el nombre de NETLOGON

Compartir una carpeta o directorio

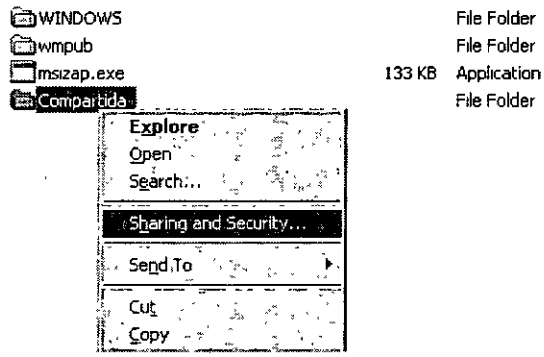
Para compartir una carpeta, se debe estar conectado como administrador y seguir los siguientes pasos (se crearan las carpetas):

1. Desde el explorador de Windows del servidor, sitúese en el directorio de donde desea colocar la carpeta que va a crear, por ejemplo colóquese en **C:**, abra el menú **File** y seleccione **New.**

De las opciones que aparecen, seleccione **Folder** e indique el nombre que tendrá el directorio; por ejemplo Publica y pulse **Enter**.

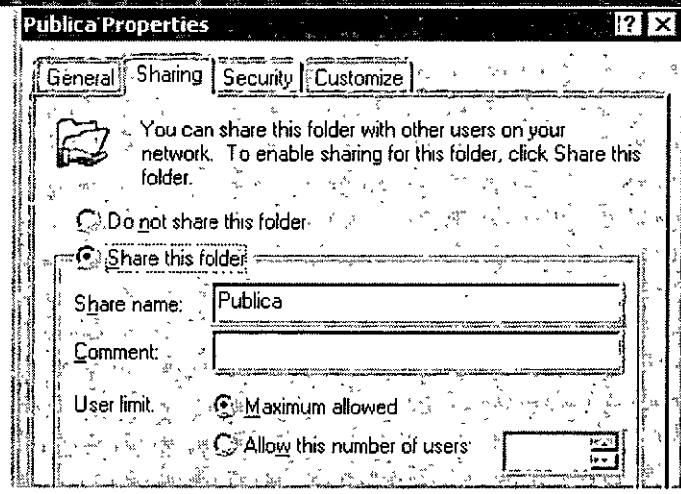


2. Sitúese sobre el nuevo directorio, pulse el botón derecho del ratón.



3. Active la casilla **Share this folder** e indique el nombre de recurso compartido que desee. En el apartado **Descripción**, indique un breve comentario para este recurso compartido.

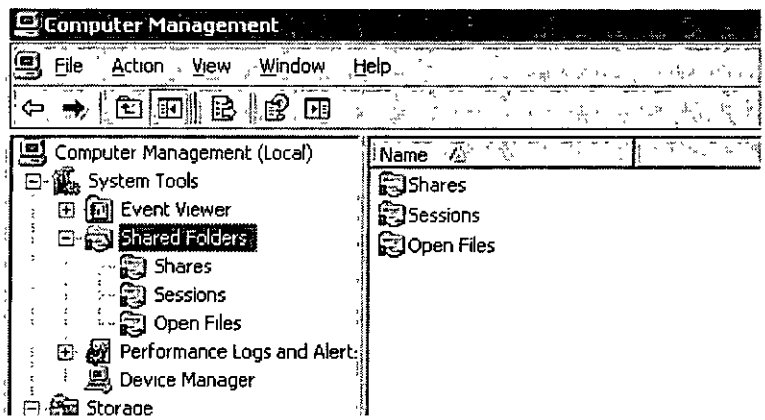
Deje activada la casilla **Maximum allowed** como límite de usuarios o active **Allow this number of users** e indique el número de usuarios que pueden conectarse simultáneamente. Cuando haya finalizado marque en **OK**.



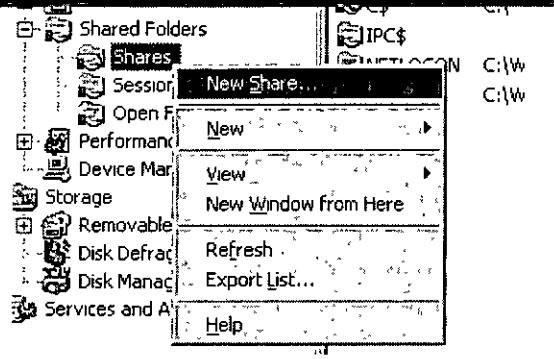
Otra opción para realizar lo anterior, es utilizando la utilidad de **Computer Managment:**

1. Seleccione **Computer Managment** de **Administrative Tools** del menú **Start**.

2. Pulse el botón izquierdo del ratón sobre el signo "**+**" ubicado junto a **Shared Folders** que se encuentra en el panel izquierdo de la ventana para desplegar su contenido: **Recursos Compartidos, Sesiones y Archivos Abiertos**.



3. Pulse el botón derecho del ratón sobre **Shares** y seleccione **New Share** del menú contextual.



4. Aparecerá un ayudante para la creación de una nueva carpeta compartida. Pulse **Siguiente** e indique la ruta de la carpeta que desea compartir, puede pulsar **Browse** para seleccionarla. Si en esta pantalla pulsa **Make New Folder**, podrá crearla previamente, pulse siguiente.

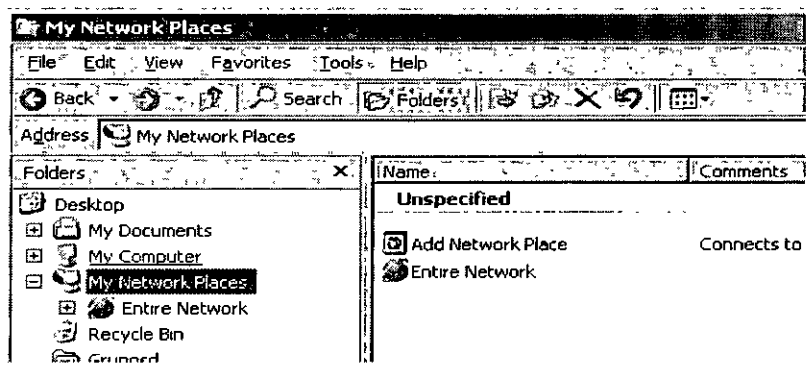
5. Indique el nombre que desea darle al recurso compartido y una breve descripción, dé en **Siguiente**.

6. Puede indicar los permisos que desee para la carpeta que acaba de compartir, cuando termine marque **Finalizar.**

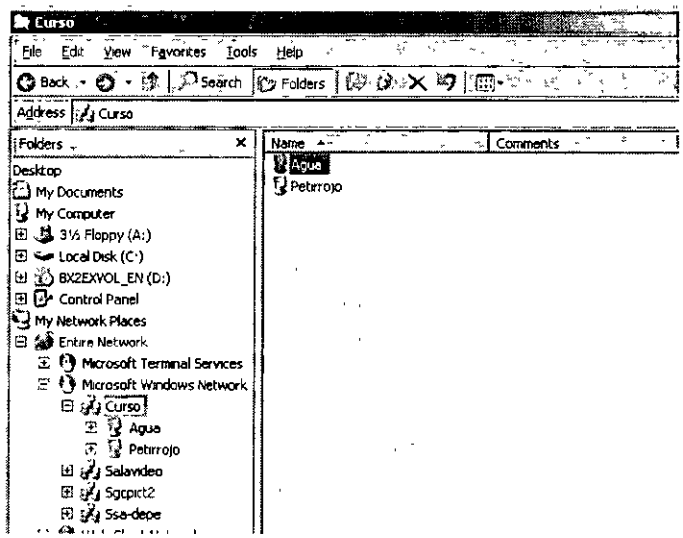
Ver los directorios compartidos

Una vez creados los directorios compartidos en el servidor, los usuarios pueden acceder a ellos utilizando dos formas diferentes:

- Desde el icono **My Network Places** en el menú **Start**.
- Desde el icono **My Network Places** que hay en el **Windows Explorer**.



En cualquiera de los dos casos, en la pantalla que se muestra, seleccione **Entire Network**, posteriormente pulse en **Microsoft Windows Network**, seleccione el dominio correspondiente, marque en el servidor que desee y le mostrará todos sus recursos compartidos.



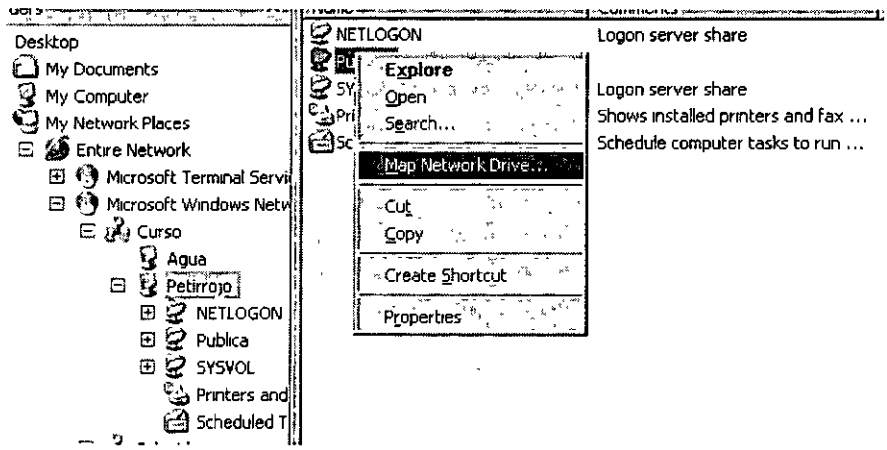
Conectarse a los directorios

Una vez que el directorio ha sido compartido, una forma fácil de conectarse a él es asignarle una letra de unidad. Esta letra, podrá ser una de las que este disponibles de la A a la Z, para poder acceder a él desde el icono **My computer**.

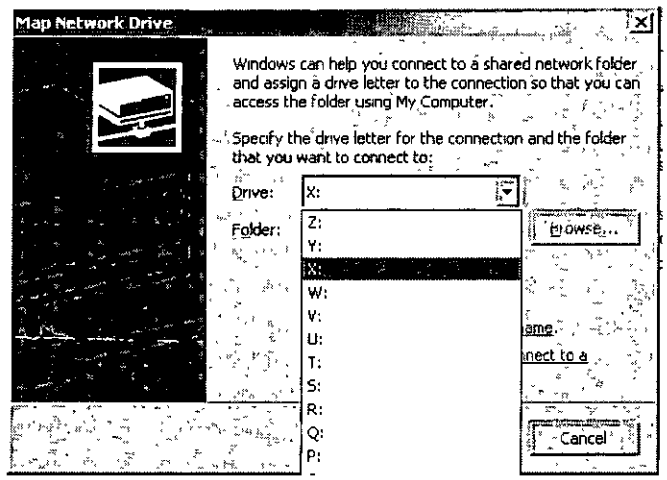
Para conectar la carpeta **Publica** a la letra **X**: siga los siguientes pasos:

1. Abra el icono **My Network Places** y siga los pasos necesarios hasta que seleccione el servidor que desee.

2. Elija un directorio compartido y pulse el botón derecho del ratón. Seleccione la opción **Map Networ Drive**.



3. Aparecerá una pantalla como la que se muestra a continuación y en la cual podrá cambiar la letra que asignará al directorio compartido.

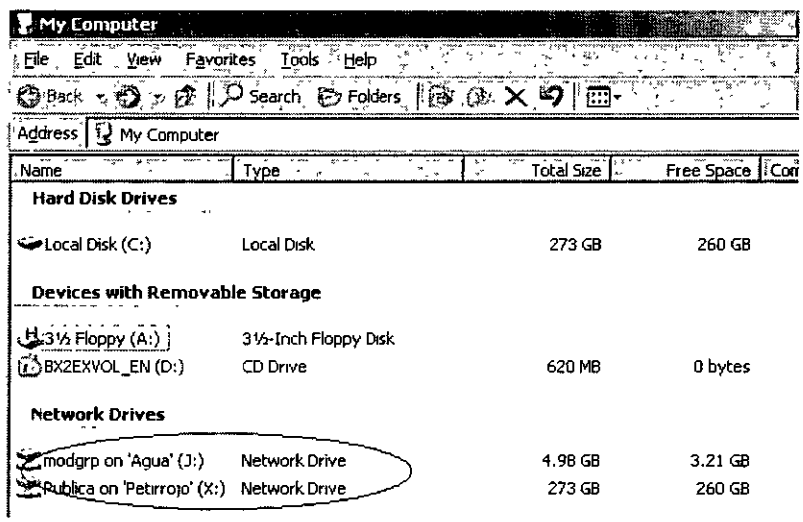


Si no tiene permiso para acceder al directorio compartido, deberá indicar en el apartado **Connect using a different user name** un nombre de usuario que sí tenga permiso para acceder a él.

Si desea volverse a conectar cuando inicie la sesión, active la casilla ***Reconnect at Logon.***

4. Una vez finalizado esto, de clic en **Finish** y se conectara al directorio para mostrarle su contenido. Cierre la ventana.

5. Puede abrir **My Computer**, y verá que aparece la letra junto al nombre del recurso compartido en el apartado **Network Drivers** y se podrá acceder a él rápidamente.



Permisos de carpetas compartidas

Cuando se establecen los permisos de una carpeta compartida, únicamente son efectivos cuando se tiene acceso a la carpeta a través de la red, es decir, no protegen a los directorios cuando se abren localmente en el servidor. Para los directorios locales deben utilizarse los permisos NTFS

Los permisos de carpetas compartidas sólo se aplican a los usuarios que acceden a las mismas desde la red y no afectan a los usuarios que accedan desde el equipo donde se encuentra la carpeta compartida. Los permisos pueden asignarse a cuentas de usuarios, grupos y cuentas de equipo.

Los permisos son:

- **Read**, es el permiso predefinido cuando compartimos una carpeta y se aplica al grupo 'todos', este permiso permite ver los nombres de archivo y nombres de subcarpetas; ver los datos del archivo y sus atributos; ejecutar archivos de programa.
- **Change**, incluye el permiso de Lectura, además permite añadir archivos y subcarpetas; cambiar los datos de los archivos; borrar archivos y subcarpetas.
- **Full Control**, todos los anteriores y además permite cambiar permisos NTFS a los archivos y a las carpetas.

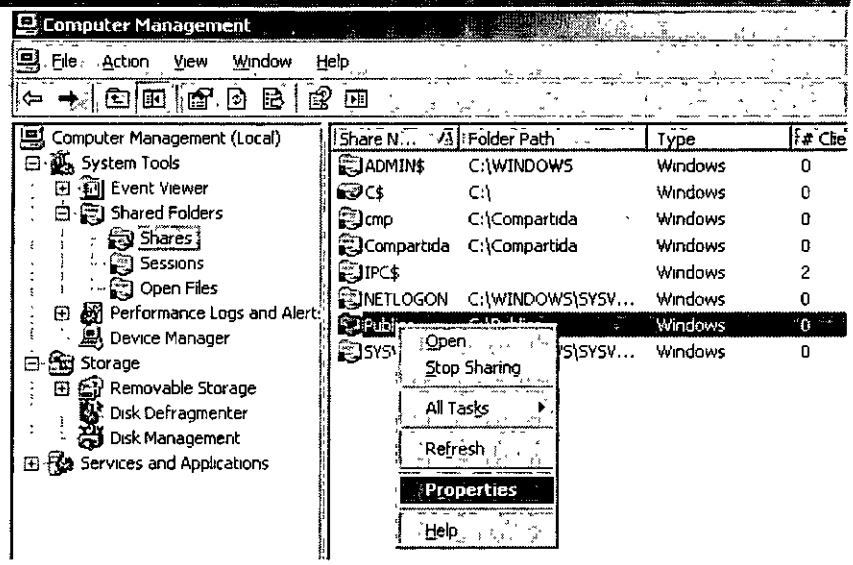
Podemos asignar los permisos a una carpeta compartida desde **Computer Managment** o desde **Windows Explorer**.

Utilizando **Computer Managment**:

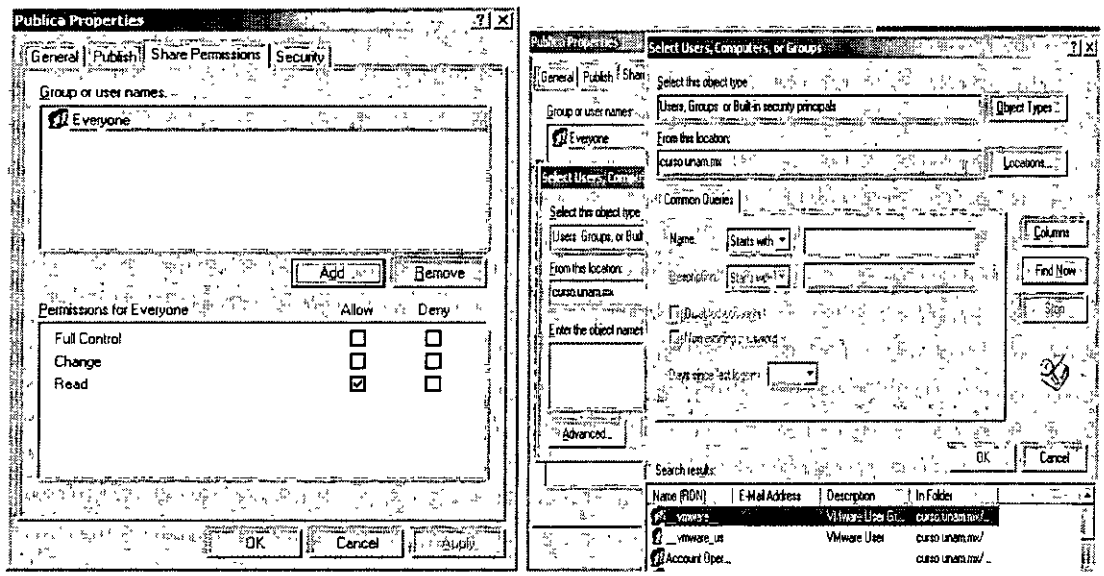
1. Seleccione **Computer Managment** de **Administrative Tools** del menú **Start**.

2. En el árbol de la consola, expandimos **Shared Folders** y pulsamos en **Shares**.

3. En el panel de detalles, de clic derecho sobre la carpeta compartida a la que quiere configurarle los permisos y pulse en **Properties**.



4. En el cuadro de diálogo de las propiedades, ficha **Share Permissions**, aquí podemos pulsar en **Add** para asignar permisos. Luego seleccionamos los usuarios, grupos o equipos y pulsamos **OK**; o pulsar en quitar para eliminar el acceso a usuarios, grupos o equipos.



Podemos dar clic en **Advanced** y luego en **Find Now** para abrir una ventana con todos los posibles usuarios, grupos o equipos a los que se pueden denegar u otorgar permisos.

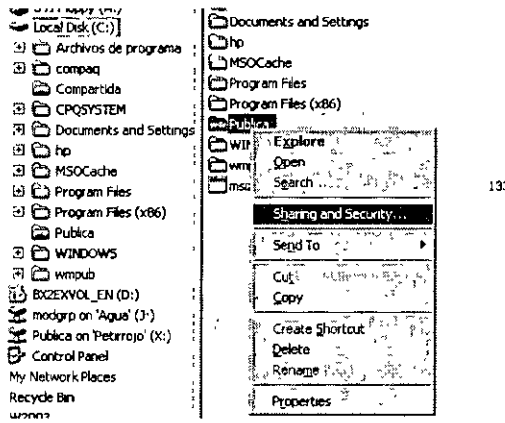
5. En el cuadro de **Permisos**, puede activar o desactivar las casillas que desee tanto de la columna **Allow** (concede el permiso correspondiente al objeto seleccionado)

como de la columna **Deny** (niega el permiso correspondiente al objeto seleccionado).

Utilizando **Windows Explorer**:

1. Abrir **Windows Explore.**

2. Clic derecho sobre la carpeta compartida para obtener su menú contextual, pulsamos en **Sharing and Security**.



3. En el cuadro de diálogo de propiedades, ficha **Share Permissions**, pulsamos el botón **permisos**.

4. Aquí es idéntico a los pasos 4 y 5 indicados anteriormente.

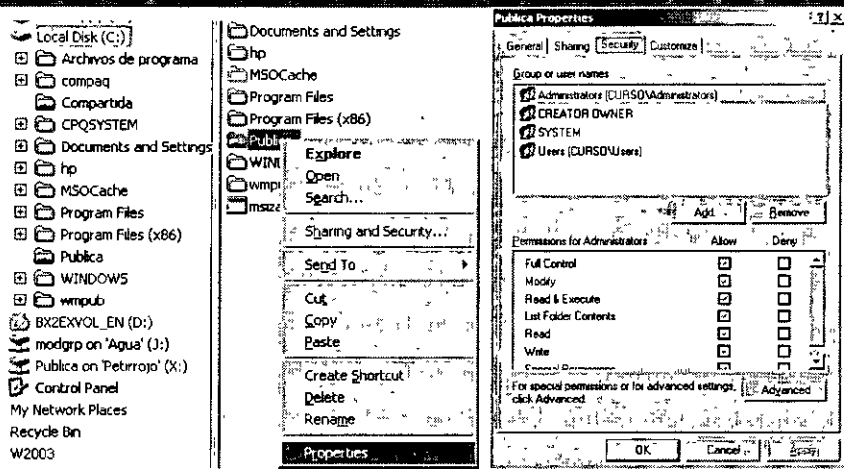
Administrar acceso a archivos y carpetas utilizando permisos NTFS

¿Cómo establecer los permisos NTFS para un archivo o una carpeta?

Para establecer los permisos NTFS para un archivo o carpeta:

1. Inicie el **Explorador de Windows** y busque el archivo o carpeta para la que desea establecer permisos.

2. Haga clic con el botón secundario del ratón en el archivo o en la carpeta, de clic en **Properties** y después haga clic en la ficha **Security**.



3. Si desea configurar los permisos para un nuevo usuario o grupo, haga clic en **Add**. En el cuadro de diálogo **Seleccionar usuarios, equipos o grupos**, escriba el nombre del usuario o del grupo para el que desee configurar los permisos, haga clic en **Chake Names** para comprobar los nombres y después dé clic en **OK**.

Podemos dar clic en **Advanced** y luego en **Find Now** para abrir una ventana con todos los posibles usuarios, grupos o equipos a los que se pueden denegar u otorgar permisos.

4. Para conceder o denegar permisos en la lista **Permissions**, haga clic en el usuario o grupo de la lista **Group or user names** y active la casilla de verificación (**Alow** o **Deny**) situada junto al permiso que desea conceder o denegar.

Los permisos estándar para directorios que se pueden conceder o denegar son:

Permiso NTFS de Directorio	Permite al usuario:
Read	Mostrar archivos y subdirectorios en el directorio y visualizar los atributos, propietario y permisos para directorio.
Write	Crear nuevos archivos y subdirectorios dentro del directorio, cambiar atributos de directorio y visualizar el propietario y permisos para directorio.
List Folder Contents	Mostrar los nombres de archivos y subdirectorios en el directorio.
Read & Execute	Recorrer directorios y las acciones permitidas por el permiso de Read y List Folder Contents.

Modify	Eliminar el directorio y realizar las acciones permitidas por el permiso de Write y Read & Execute.
Full Control	Cambiar los permisos, tomar propiedad, eliminar subdirectorios y archivos y realizar las acciones permitidas por todos los demás permisos NTFS de directorios.

5. O bien, para quitar al grupo o usuario, haga clic en el usuario o grupo de la lista **Group or user names** y a continuación, haga clic **en Remove**. Haga clic en **OK.**

Establecer permisos especiales

Puede configurar cualquiera o todos los permisos especiales siguientes para archivos y carpetas.

Recorrer carpeta o ejecutar archivo

Para carpetas: el permiso **Recorrer carpeta** permite o impide que el usuario pase de una carpeta a otra para llegar a otros archivos o carpetas, incluso aunque el usuario no tenga permisos para las carpetas recorridas (sólo se aplica a carpetas). **Recorrer carpeta** sólo surte efecto cuando al grupo o al usuario no se le ha concedido el permiso **Omitir comprobación de recorrido**, que comprueba los derechos de usuario en el complemento Directiva de grupo. De manera predeterminada se concede al grupo **Todos** el derecho de usuario **Omitir comprobación de recorrido**.

Para archivos: el permiso **Ejecutar archivos** permite o deniega los archivos de programa que hay en ejecución (sólo se aplica a archivos).

Al configurar el permiso **Recorrer carpeta** en una carpeta, no se configura automáticamente el permiso **Ejecutar archivo** en todos los archivos de dicha carpeta.

Listar carpeta / Leer datos

El permiso **Listar carpeta** permite o impide que el usuario vea los nombres de archivo y de subcarpeta en la carpeta. El permiso **Listar carpeta** sólo afecta al contenido de dicha carpeta, no a si se muestra o no el contenido de la carpeta para la que está configurando el permiso. Esto se aplica sólo a carpetas.

El permiso **Leer datos** permite o impide ver datos de archivos (sólo se aplica a archivos).

Atributos de lectura

El permiso **Atributos de lectura** permite o impide que el usuario vea los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

Atributos extendidos de lectura

El permiso **Atributos extendidos de lectura** permite o impide que el usuario vea los atributos extendidos de un archivo o de una carpeta. Los atributos extendidos están definidos por los programas y pueden variar de uno a otro.

Crear archivos / Escribir datos

El permiso **Crear archivos** permite o impide al usuario crear archivos en la carpeta (se aplica sólo a carpetas).

El permiso **Escribir datos** permite o impide que el usuario haga cambios en el archivo y sobrescriba contenido existente (se aplica sólo a archivos).

Crear carpetas / Anexar datos

El permiso **Crear carpetas** permite o impide al usuario crear carpetas en la carpeta (se aplica sólo a carpetas).

El permiso **Anexar datos** permite o impide que el usuario haga cambios en el final del archivo pero que no cambie, elimine ni sobrescriba datos existentes (se aplica sólo a archivos).

Atributos de escritura El permiso

Atributos de escritura permite o impide que el usuario cambie los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

El permiso **Atributos de escritura** no implica la creación o eliminación de archivos o carpetas, sólo incluye el permiso para hacer cambios en los atributos de un archivo o de una carpeta. Para permitir o denegar operaciones de creación o eliminación, consulte **Crear archivos / Escribir datos, Crear carpetas /Anexar datos, Eliminar subcarpetas y archivos y Eliminar**.

Atributos extendidos de escritura

El permiso **Atributos extendidos de escritura** permite o impide que el usuario cambie los atributos extendidos de un archivo o de una carpeta. Los atributos extendidos están definidos por los programas y pueden variar de uno a otro.

El permiso **Atributos extendidos de escritura** no implica que el usuario pueda crear o eliminar archivos o carpetas, sólo incluye el permiso para hacer cambios en los atributos de un archivo o de una carpeta. Para permitir o denegar operaciones de creación o eliminación, consulte las secciones ***Crear archivos / Escribir datos, Crear carpetas / Anexar datos,*** **Eliminar subcarpetas archivos y** ***Eliminar.***

Eliminar subcarpetas y archivos

El permiso **Eliminar subcarpetas y archivos** permite o impide que el usuario elimine subcarpetas y archivos, incluso aunque no se haya concedido el permiso **Eliminar** para la subcarpeta o el archivo. Este permiso se aplica sólo a las carpetas.

Eliminar

El permiso **Eliminar** permite o impide que el usuario elimine el archivo o la carpeta. Si no tiene el permiso **Eliminar** para un archivo o una carpeta, puede eliminarlo si se le han concedido los permisos Eliminar subcarpetas y archivos en la carpeta principal.

Leer permisos

El permiso **Leer permisos** permite o impide que el usuario lea permisos del archivo o de la carpeta, como **Control total, Leer y Escribir**.

Cambiar permisos

El permiso **Cambiar permisos** permite o impide que el usuario cambie permisos del archivo o de la carpeta, como **Control total, Leer y Escribir**.

Tomar posesión

El permiso **Tomar posesión** permite o impide que el usuario tome posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta puede cambiar los permisos correspondientes, cualesquiera que sean los permisos existentes que protegen el archivo o la carpeta.

Sincronizar

El permiso **Sincronizar** permite o impide que distintos subprocesos esperen en el controlador del archivo o de la carpeta y se sincronicen con otro subproceso que pueda señalarlos. Este permiso se aplica únicamente a programas multiproceso de múltiples subprocesos.

Configurar, ver, cambiar o quitar permisos especiales de archivos y carpetas

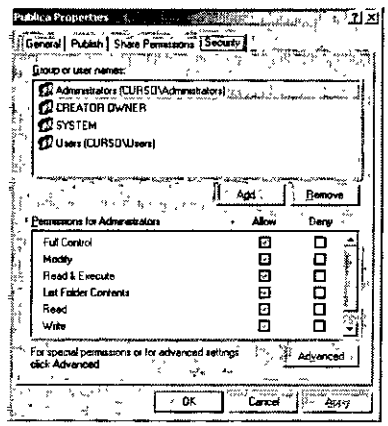
Para configurar, ver, cambiar o quitar permisos especiales para archivos y carpetas:

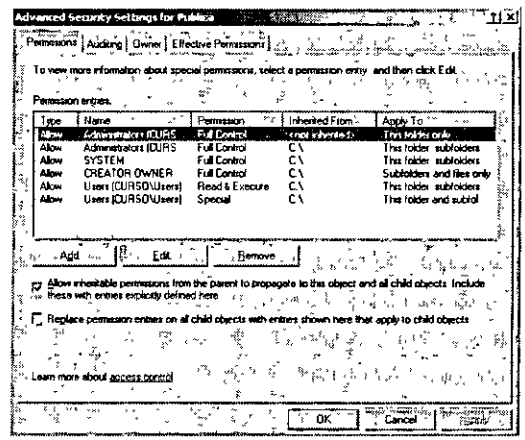
1. Seleccione ***Computer Managment*** de ***Administrative Tools*** del menú **Start**.

2. En el árbol de la consola, expandimos **Shared Folders** y pulsamos en **Shares**.

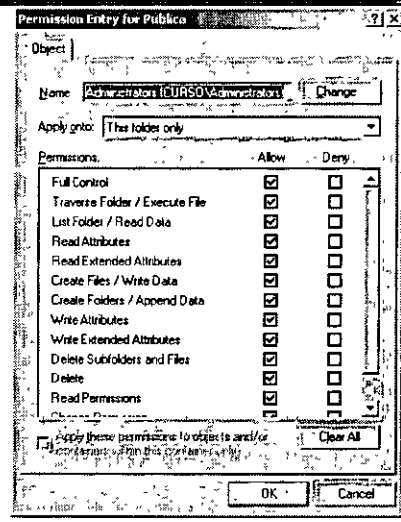
3. En el panel de detalles, clic derecho sobre la carpeta compartida a la que quiere configurarle los permisos y pulsamos en **Properties**.

4. Seleccione la ficha **Security** y marque **Advanced**, se mostrará una pantalla en la que se encuentran los nombres de los usuarios, grupos y equipos especiales que tienen permisos sobre dicho directorio o archivo junto con una descripción de los permisos y dónde se aplican.





5. Si desea modificar los permisos de alguno de ellos, sitúese sobre él y de clic en **Edit**, se mostrara la pantalla siguiente



En esta pantalla se muestran los permisos especiales que tiene establecidos el usuario o grupo seleccionado. Si existen casillas en gris, significa que son permisos heredados.

6. Puede modificar los permisos que desee. Para esto, active la casilla correspondiente al permiso deseado en la columna **Allow** (concede el permiso) o **Deny** (se le deniega el permiso).

7. Puede indicar en el apartado **Apply onto**, el ámbito de los permisos que está indicando, puede modificar al ámbito desplegando la lista.

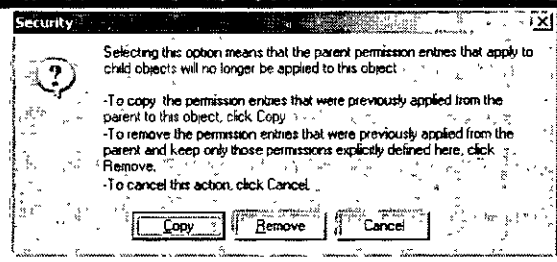
   Si activa **Apply onto this folder only** evitará que los archivos y subcarpetas secundarias hereden estos permisos. Una vez que haya terminado, dar clic en **OK**.

8. Si se desean añadir otros usuarios o grupos a la lista de nombres, dar clic en **Add,** pulsar en **Advanced** y pulsar en **Fin Now**. Se abrirá una ventana con todos los posibles usuarios, grupos y computadores a las que puede otorgar o denegar permisos.

   Si desea quitar algún usuario o grupo, colóquese sobre él, dar clic en **Remove**.

9. Si quiere que los permisos de la carpeta principal no sean heredados a esta carpeta secundaria, asegúrese en qué hay casillas de permisos que pueden estar en gris porque son permisos heredados, desactive la casilla **Allow inheritable permissions from the parent to propágate to this object and all child objects...**

   Aparecerá la pantalla siguiente:



-Si se marca la opción **Copy**, concederá al objeto los permisos que tenía el objeto principal y podrán ser modificados.
-Si se marca la opción **Remove**, el objeto no heredará los permisos del objeto principal y podrán añadirse nuevos permisos.

10. Si quiere que los permisos indicados para esta carpeta se heredan a todos los subdirectorios secundarios, active la casilla **Replace permission entries on all child objects with entries shown here that apply to child objects.** Después dar clic en **OK** y se mostrará un cuadro de diálogo que indica que se eliminarán los permisos indicados en los subdirectorios y archivos que cuelgan de este directorio. Dar clic en **Yes** para continuar.

11. Una vez terminados los cambios a los permisos, dar clic en **OK** para regresar a la pantalla de Propiedades del directorio. Dar clic en **Ok** en la utilidad.

Determinar permisos eficaces

¿Cuáles son los permisos NTFS efectivos en archivos o carpetas?

En general:

- Los permisos son acumulativos
- Los permisos de los archivos preceden a los de las carpetas.
- Denegar siempre sobrescribe todos los permisos.
- Se puede tomar la propiedad.

Los permisos eficaces de un usuario para un recurso, son la combinación de los permisos compartidos de la carpeta que concedes a la cuenta individual del usuario y a los permisos compartidos de la carpeta que concedes a los grupos a los que el usuario pertenece.

Por ejemplo: Si un usuario ha leído el permiso de tener acceso a la carpeta, pero también un miembro de un grupo que tiene el permiso de escritura para la misma carpeta, después el usuario consigue leído y los permisos de escritura para esa carpeta.

Windows Server 2003 ® nos ofrece una herramienta para mostrarnos los permisos efectivos, que son la unión de los permisos basada en la pertenencia del usuario a grupos.

La información se extrae desde las entradas existentes y son mostrados en un formato de solo lectura.

Los permisos efectivos tienen las siguientes características:

- Los permisos acumulados son una combinación de los permisos concedidos al usuario y a todos los grupos de los que es miembro.
- Los permisos de archivos siempre tienen precedencia sobre los de la carpeta. denegar sobrescribe todos los permisos.
- Cada objeto tiene un propietario en Active Directory. El propietario controla como se configuran los permisos en el objeto y a quien se le conceden.

Nota:

Un Administrador que necesite reparar o cambiar permisos en un archivo debe tomar posesión del archivo.
De manera predefinida en Windows Server 2003 ® el propietario es el grupo administradores. El propietario puede también cambiar permisos en un objeto aún cuando se haya denegado todo el acceso al objeto.

La propiedad (o posesión) puede tomarse por:

- Un administrador. De manera predefinida, el grupo administradores tiene dado el derecho a tomar la posesión de archivos u otros objetos.
- Cualquiera o cualquier grupo que tiene el permiso 'tomar posesión' para el objeto en cuestión.
- Un usuario que tiene el privilegio de **'Restaurar archivos y directorios'**.

La propiedad puede ser transferida mediante los siguientes métodos:
El actual propietario puede conceder el permiso 'tomar posesión' a otro usuario. El usuario debe tomar posesión para completar la transferencia.
Un Administrador puede tomar la posesión.
Un usuario que tiene el privilegio de **'Restaurar archivos y directorios'** puede con doble clic sobre 'otros usuarios y grupos' elegir cualquier usuario o grupo para asignarles la propiedad.

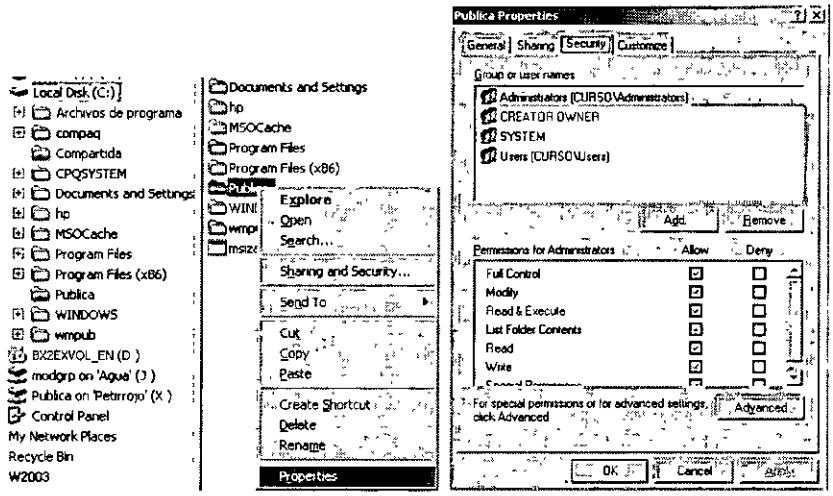
Nota:

Los permisos de una carpeta compartida no son parte del cálculo de permisos efectivos. El acceso a una carpeta compartida puede estar denegado aún cuando el acceso esté permitido con NTFS.

Ver permisos efectivos de archivos y carpetas

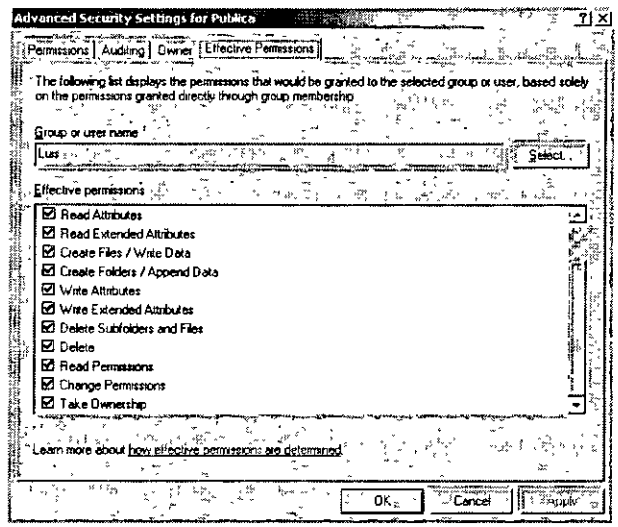
1. Inicie el **Explorador de Windows** y a continuación, busque el archivo o carpeta para la que desea establecer permisos.

2. Haga clic con el botón secundario del ratón en el archivo o en la carpeta, haga clic en **Properties** y haga clic en la ficha **Security**.



3. Haga clic en **Advanced**, después clic en la ficha **Effective Permissions** y a continuación en **Select.**

4. En **Goup or user name**, escriba el nombre de un usuario o grupo y, después, haga clic en ***OK.*** Las casillas de verificación activadas indican los permisos efectivos del usuario o grupo para ese archivo o carpeta



En la ficha **Effective Permissions** se muestra información que se calcula a partir de las entradas de permisos existentes. Por lo tanto, la información presentada en esa página es de sólo lectura y no admite cambiar los permisos de un usuario con la activación o desactivación de las casillas de verificación de permisos.

Administrar acceso a archivos compartidos utilizando la Caché sin conexión implementar la impresión.

Para hacer que los archivos y programas de red compartidos estén disponibles sin conexión, Archivos sin conexión almacena una versión de los mismos en una memoria caché. El equipo puede tener acceso a esta memoria caché cuando no esté conectado a la red. Se puede elegir entre tres opciones de almacenamiento en caché al compartir archivos:

- Sólo estarán disponibles sin conexión los programas y archivos que especifique el usuario
  Esta opción de almacenamiento en caché proporciona acceso sin conexión a solamente los archivos y programas identificados específicamente por un usuario que utilice la carpeta compartida. Es la opción ideal para una carpeta de red compartida con archivos y programas a los que tendrán acceso y serán modificados por varias personas. Ésta es la opción predeterminada cuando se configura una carpeta compartida para ser usada sin conexión.

- Todos los programas que el usuario abra desde el recurso compartido estarán disponibles sin conexión automáticamente

  Esta opción de almacenamiento en caché hace que todos los archivos y programas abiertos en la carpeta compartida estén disponibles sin conexión automáticamente. Los archivos y programas sin abrir no están disponibles sin conexión. Es la opción de almacenamiento en caché ideal para hacer que estén disponibles sin conexión archivos y programas que se leen, a los que se hace referencia o se ejecutan, pero no se modifican en el proceso.

  El almacenamiento automático en caché de archivos y programas proporciona acceso sin conexión a carpetas compartidas con archivos y programas que no se van a modificar. El almacenamiento automático en caché de programas reduce el tráfico en la red porque los archivos sin conexión se abren directamente, sin que sea necesario tener acceso a las versiones de la red, y generalmente se inician y se ejecutan más rápido que las versiones de la red. Para proporcionar únicamente almacenamiento en caché de archivos, desactive la casilla de verificación Rendimiento óptimo.

  Si utiliza el almacenamiento automático en caché de archivos y programas, asegúrese de restringir los permisos de los archivos y programas contenidos en la carpeta compartida a acceso de sólo lectura.

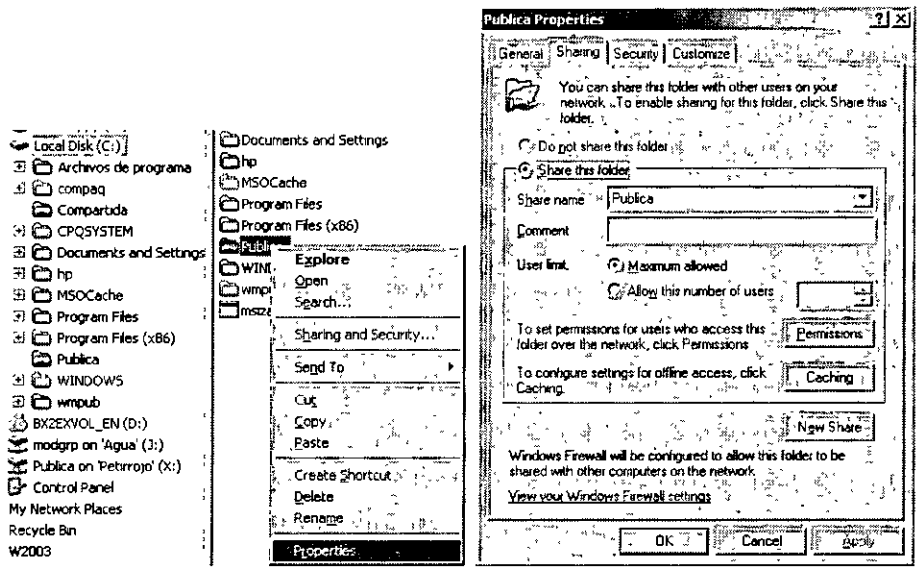
- Los archivos o programas desde el recurso compartido no estarán disponibles sin conexión

- Los archivos o programas de la carpeta compartida no estarán disponibles sin conexión.

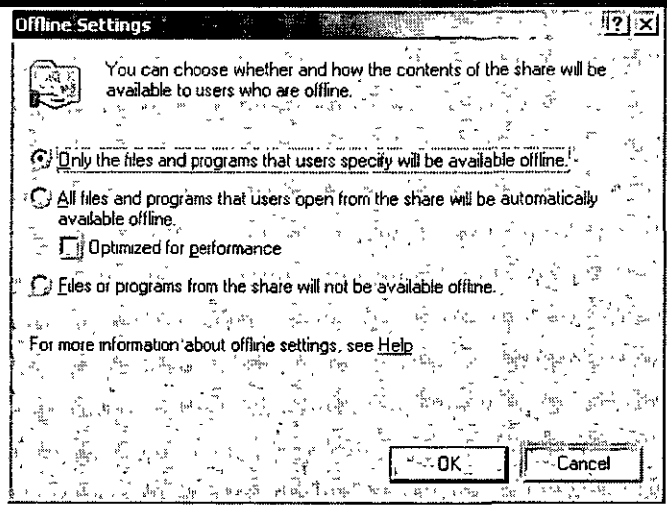
Acceso a archivos compartidos utilizando la Caché sin conexión

1. Inicie el **Explorador de Windows** y busque el archivo o carpeta para la que desea establecer permisos.

2. Haga clic con el botón secundario del ratón en el archivo o en la carpeta, haga clic en **Properties** y haga clic en la ficha **Sharing.**



3. Dar clic en el botón **Caching** y se mostrara la pantalla siguiente:



4. Elegir la opción que se desea. Y dar **OK**

WINDOWS 2003 SERVER ®

Tema 6

Introducción a la impresión en Windows 2003 ®

- Instalar y compartir impresoras
- Administrar acceso a las impresoras utilizando permisos de impresoras a compartir
- Administrar controladores de impresión
- Implementar la ubicación de las impresoras

FLORES ALVAREZ LUIS ARMANDO
GUERRERO MARTÍNEZ EDSON ARMANDO

Instalar y compartir impresoras

Una **impresora** propiamente dicha es la máquina en la que se va a producir físicamente la impresión de un trabajo. Puede dar soporte a una o varias colas de impresión. Es importante distinguir entre impresora e impresora lógica que es equivalente a la cola de impresión.

Una **cola de impresión** es un archivo en el que se van a guardar los trabajos que se manden a imprimir hasta que la impresora pueda darles salida. Puede dar soporte a una o varias impresoras (es lo que se hace al agregar una impresora). De manera predeterminada, la carpeta donde se guardan los archivos de cola de impresión se encuentra en \WINDOWS\system32\spool\PRINTERS. Si el servidor de impresión únicamente sirve a una o dos impresoras con un volumen de tráfico reducido, esta ubicación predeterminada será suficiente, pero si se requiere un volumen elevado de impresión, por haber un gran número de impresoras o trabajos de impresión de gran tamaño, será conveniente cambiar la ubicación de la carpeta.

Un **servidor de impresión** es una computadora, servidor o estación de trabajo, en el que esta conectada físicamente la impresora y que se encarga de solicitar a la cola de impresión que le envíe los trabajos cuando ésta esté disponible. Puede dar soporte a varias impresoras y a varias colas de impresión.

Ventajas de un servidor de impresión

- Administra la configuración del controlador de impresión
- Para todos los equipos que estén conectados a una impresora únicamente aparece una cola de impresión, lo que permite a los usuarios ver la posición de su trabajo de impresión respecto a los demás trabajos en espera
- Los mensajes de error aparecen en todos los equipos, por lo que todos los usuarios conocen el verdadero estado de la impresora.
- Parte del proceso de impresión se transfiere del equipo cliente al servidor de impresión por lo que aumenta la capacidad de trabajo de la estación.
- Se puede establecer un registro único para aquellos administradores que deseen auditar los sucesos de la impresora.

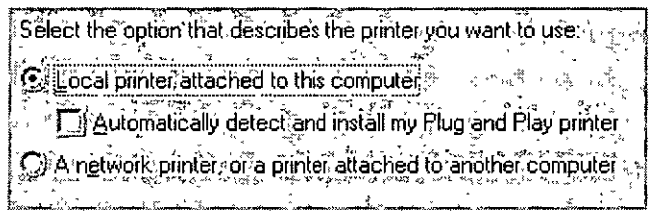
Un **controlador de impresora** es un programa de software que utiliza los programas para comunicarse con las impresoras, convirtiendo la información enviada desde el equipo a comandos que puedan entender cada impresora. Normalmente, los controladores de impresora no son compatibles entre las distintas plataformas, por lo que se deben de instalar diversos controladores en cada servidor de impresión para admitir diferentes componentes de hardware y sistemas operativos.

Para poder utilizar una impresora física, es necesario crear una impresora en Windows 2003 Server ® que tenga los controladores necesarios para poder utilizarla. Este proceso puede hacerlo un usuario que tenga el permiso de **Manage Printers**, por defecto lo tienen todos lo usurarios que pertenezcan a un grupo de **Administrators, Server Operators** o **Printer Operators.**

Una vez que se haya conectado la impresora al puerto correspondiente del equipo, siga los pasos siguientes:

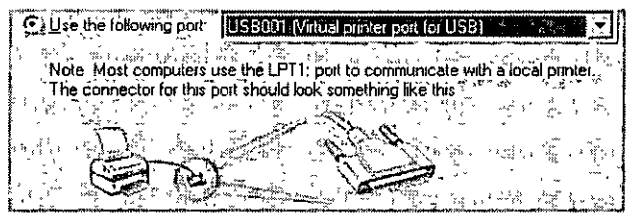
1. Ejecute el icono **Printers and Faxes**, que se encuentra en el **Control Panel** y después **Add Printer.**

2. Nos llevará a **Add Printer Wizard**, marque **Next** y le mostrará la pantalla en donde debe de elegir **Local printer attached to this computer,** la cual es la opción a elegir porque la impresora estará en este equipo y dé clic en **Next.**

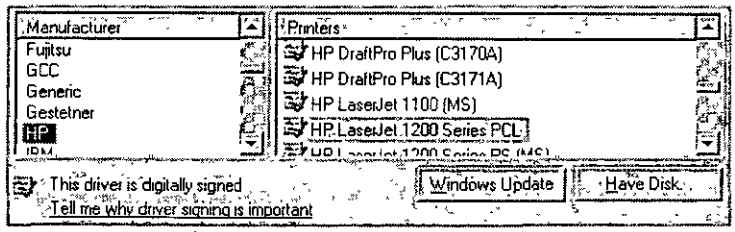


En la casilla de **Automatically detect and install my Plug and Play printer** según sea el caso se deberá marcar o no, en caso afirmativo el sistema intentará detectar la impresora y si la encuentra la instalará. En el caso contrario el proceso se realizará de forma manual.

3. Entonces aparecerá la pantalla en donde se debe de indicar el puerto local donde esta conectada la impresora. Se pueden añadir nuevos puertos si es necesario. **Next.**

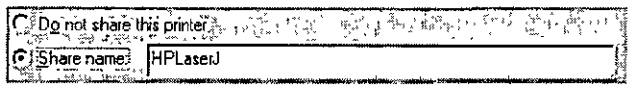


4. Ahora deberá escoger la impresora que esta conectada a dicho puerto para que se carguen los drivers. Elegir el fabricante y nombre de la impresora. En el caso de que no se encuentre y que se cuente con los drivers, podemos utilizar la opción de **Have Disk. Next.**



5. La siguiente ventana le pedirá el nombre de la impresora. **Next.**

6. En la nueva pantalla deberá indicar si la impresora estará compartida o no. Si decidimos compartirla deberemos indicar el nombre de la impresora. **Next.**

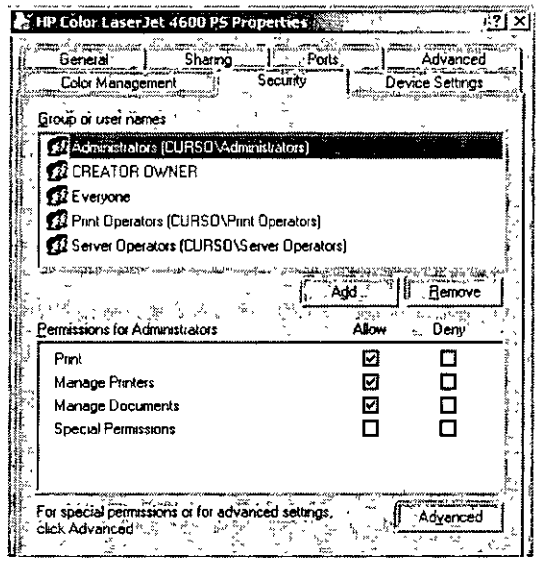


7. Después se mostrará una pantalla en donde se deberá especificar la ubicación de la impresora y una breve descripción. **Next.**

8. Por último le pregunta si quiere imprimir una página de prueba, marcar y dar clic en **Next**; para pasar a la página resumen de configuración y marcar Finalizar. Después de esto se empezará con la impresión de la página de prueba si se seleccionó.

Administrar acceso a las impresoras utilizando permisos de impresoras a compartir

Para administrar el acceso a las impresoras utilizando permisos de impresoras a compartir es necesario ir a **Printers and Faxes** que se encuentra en el menú de **Start**. Al abrir esta ventana aparecerá la impresora que tenemos instalada, al seleccionarla en su menú contextual aparecerá la opción de **Properties** en donde iremos a la pestaña de **Security**



Aquí se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos sobre el objeto y debajo los permisos estándar que posee cada uno de ellos. Hay tres tipos de permisos estándar de impresora: **Print, Manage Printers** y **Manage Documents**. De manera predeterminada todos los usuarios tienen concedido el permiso **Print** como miembros de **Everyone.**

Para trabajar con los permisos estándar sobre las impresoras, siga lo siguientes pasos:

1. Si desea modificar los permisos de alguno de ellos, sitúese sobre él y verá que en la parte inferior, se muestran los permisos que tiene establecidos. Para ello active la casilla correspondiente al permiso deseado en la columna **Allow** o **Deny.**

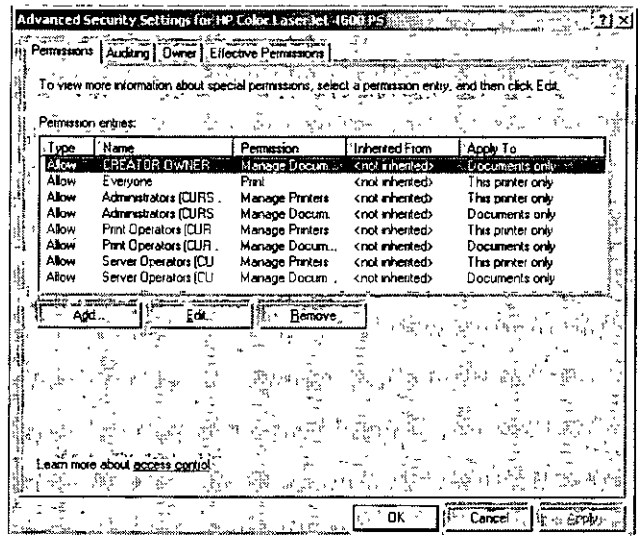
2. Si desea añadir otros usuarios o grupos a la lista de nombres, marque en **Add**, pulse en **Advanced** y pulse en **Find now**. Se le abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a las que se les puede otorgar o denegar permisos.

Si selecciona elementos de la lista dar clic en **OK** dos veces y se añadirá el objeto seleccionado. Una vez que este en la lista indique los permisos que desea conceder o denegar.

3. Si desea quitar algún usuario o grupo, sitúese sobre él, y maque en **Remove** y verá como se elimina de la lista.

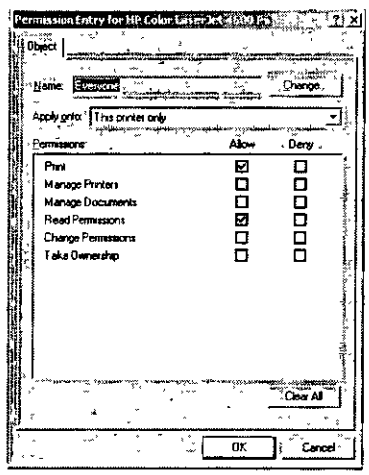
Para trabajar con permisos especiales sobre las impresoras, siga los siguientes pasos:

1. Marque en **Advanced** en la pestaña de **Security** en **Properties** de la impresora seleccionada.



En ella se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos especiales sobre la impresora junto con una descripción de los permisos y donde se aplican.

2. Si desea modificar los permisos de algunos de ellos, sitúese sobre él y pulse sobre **Edit.** Verá la pantalla siguiente



Note que muestra los permisos especiales que tiene establecidos el usuario o el grupo seleccionado.

3. Puede modificar los permisos que desee. Para ello, active la casilla correspondiente al permiso deseado en la columna **Allow** o **Deny.** Indique **OK** y luego **Apply** en el ámbito de permisos que esta indicando.

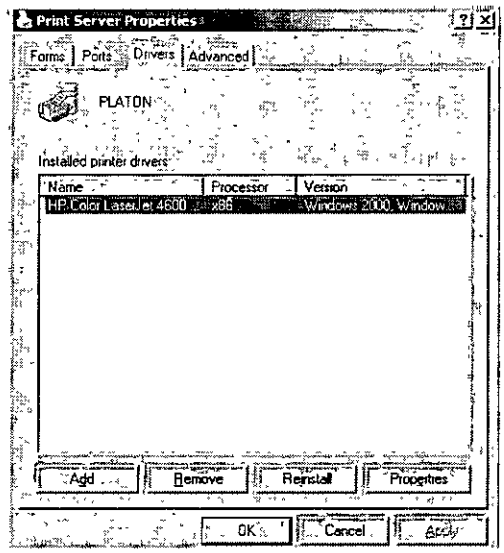
5. Si desea añadir otros usuarios o grupos a la lista de nombres, marque en **Add** luego en **Advanced** y **Find now**. Se abrirá una ventana con todos lo posibles usuarios, grupos e identidades especiales a las que se les puede otorgar o denegar permisos.

6. Si desea quitar usuario o grupo, solo sitúese sobre él y de clic en **Remove.**

7. De clic en **OK.**

Administrar Controladores de impresión

En la opción de **Server Properties** del menú de **File** abrirá una ventana en donde se encuentra la pestaña de **Drivers,** y verá la siguiente pantalla:



En ella se muestran los controladores de impresora instalados en el servidor de impresión, el entorno y la versión de dichos controladores. Se pueden realizar las siguientes tareas:

- Si desea añadir otro, marque en **Add** y entrará en el asistente. Marque en **Next,** indique el fabricante y la impresora, de clic en **Next** indique el entorno y la versión, clic en **Next** y después en Finalizar.

- Si desea remplazar un driver existente, selecciónelo, marque en **Reinstall** y confirme que desea realizarlo.

- Si desea ver los datos del controlador, selecciónelo, pulse en **Properties** y mostrará información sobre el driver, así como los archivos correspondientes. Si se sitúa sobre uno de los archivos y pulsa en **Properties**, verá datos sobre dicho archivo. Cuando haya finalizado marque en **OK** y volverá a la pantalla de **Properties** del **Printer Server**.

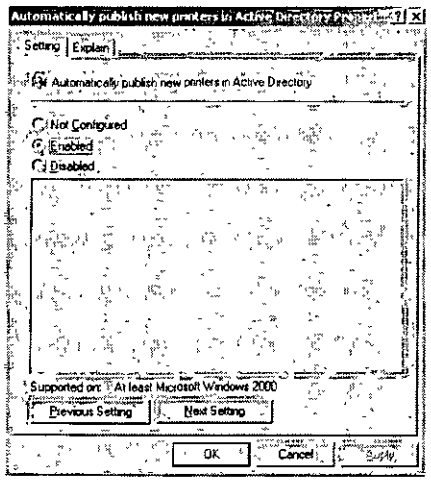
- Si desea eliminar un driver existente, selecciónelo, pulse en **Remove** y confirme que desea realizarlo.

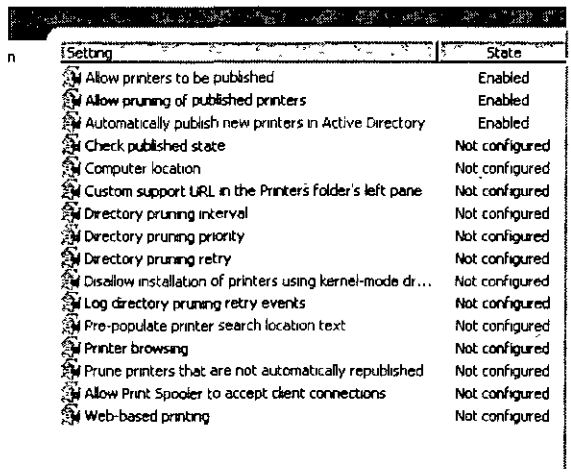
Implementar la ubicación de las impresoras

La publicación de impresoras hace posible su búsqueda en el Directorio Activo de las impresoras, así facilita su localización y su utilización.

Para establecer o modificar las opciones de publicación de las impresoras compartidas en el Directorio Activo, se han de habilitar varias directivas de la opción Impresoras del apartado Plantillas administrativas referidas a la Configuración del equipo desde una Directiva de grupo.

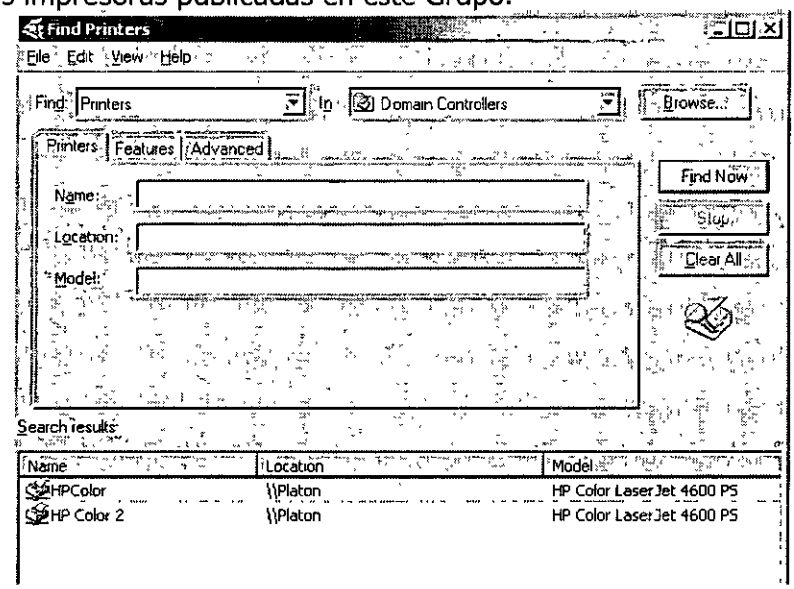
1. Abrir la consola de **Active Directory Users and Computers**, del menú de **Administrative tools** en menú **Start**.
2. Seleccionar una directiva de grupo, desde la pestaña de **Properties** del menú contextual de un objeto de grupo, por ejemplo del Active Directory.
3. Seleccionar la directiva y editarla
4. Ir la opción de **Administrative Templates** y luego **Printers**
5. Habilitar los valores de:
   - Allow printers to be Publisher
   - Allow pruning of published printer
   - Automatically publish new printers in Active Directory





6. Después de haber habilitado estos valores cerrar la consola de edición de **Group Policy** y abrir la consola de **Active Directory** para su búsqueda.
7. Dentro de la consola de **Active Directory Users and Computers** y seleccionando el objeto donde se habilitó la publicación de impresoras del menú de **Action**, seleccionar **Find**.

8. Buscar las impresoras publicadas en este Grupo.



WINDOWS 2003 SERVER®

Tema 7

Administración de la Impresión

- Cambiar de ubicación de la cola de impresión
- Establecer prioridades de impresión
- Programar la disponibilidad de la impresora
- Configurar un conjunto de impresoras

FLORES ALVARES LUIS ARMANDO
GUERRERO MARTÍNEZ EDSON ARMANDO

Cambiar de ubicación de la cola de impresión

De forma predeterminada, la carpeta de cola de impresión se encuentra en raíz del Sistema **\System32\Spool\Printers**. Sin embargo, esta unidad también almacena los archivos de sistema de Windows. El sistema operativo utiliza con frecuencia estos archivos, por lo que es posible que el rendimiento de las funciones de impresión y de Windows disminuya.

Si el servidor de impresión sólo sirve a una o dos impresoras con un volumen de tráfico reducido, la ubicación predeterminada de la carpeta de cola de impresión será suficiente. Sin embargo, si se requiere un volumen elevado de impresión para admitir un gran número de impresoras o trabajos de impresión de gran tamaño, tendrá que cambiar la ubicación de la carpeta. Para obtener los mejores resultados, mueva la carpeta de cola de impresión a una unidad que tenga controlador propio, lo que reducirá el efecto de la impresión en el resto del sistema operativo.

¿Por qué cambiar la ubicación de la cola de impresión?

El cambiar la ubicación de la cola de impresión nos sirve para:

Mejorar el rendimiento

Los servidores de impresión deben tener suficiente espacio de disco y RAM para gestionar los trabajos de impresión. Lo ideal, es tener al menos dos discos como mínimo, uno para el sistema operativo, archivos de inicio y el archivo de paginación; otro para albergar la carpeta de la cola de impresión. Esto aísla la carpeta de la cola del sistema operativo, que mejora el rendimiento y la estabilidad. Para mejorar la eficiencia, añada un disco para el archivo de paginación.

Resolver problemas de espacio en disco

Los servidores de impresión generan una cola de impresión para gestionar las solicitudes de impresión. Los documentos pueden llegar a tener 20 MB (o más) de tamaño si incluyen gráficos. Como resultado, debería utilizarse otro disco diferente del usado por el sistema. Esto ayuda a que no se utilice todo el espacio libre del disco del sistema o partición de inicio, que pueden causar dificultades con el archivo de paginación. Si configuramos la cola de impresión en el mismo disco, Windows ® podría llegar a no tener suficiente espacio para escribir en el archivo de paginación, con lo que se provocan problemas en el rendimiento global de la impresión.

Reducir la fragmentación en la partición de inicio

Cuando se imprime un archivo en una impresora de red, se crea un archivo de cola y se elimina inmediatamente después de haberlo impreso.

Este proceso se repite cientos de veces o quizás miles durante un día normal de trabajo. Si la carpeta de cola está en un volumen compartido con otro tipo de datos, el volumen sufre una gran fragmentación. Puedes eliminarla si ubicas la carpeta de cola en un volumen completamente dedicado a la impresión. Después de que todos los trabajos se imprimen, se eliminarán desde el volumen nuevos trabajos de impresión pueden iniciarse en un disco limpio.

Asegurar seguridad

Si los trabajos de impresión están configurados para no ser eliminados después de imprimirse, se tiene la ventaja al tener los trabajos en un disco o volumen distinto y así no heredar ningún cambio en la seguridad de ninguna carpeta padre. También es ventajoso mover la cola de impresión para impresoras que imprimen datos sensibles, como la nomina o informes financieros, y así puedes auditar todas las transacciones en el disco que la contiene.

Administrar cuotas de disco

En el disco que contiene el sistema operativo no suelen configurarse cuotas de disco para incrementar el rendimiento. Sin embargo, puedes querer limitar el total de espacio de trabajos de impresión que usuarios o grupos envían al servidor de impresión y así, que un usuario no pueda ocupar el total de espacio libre disponible en el servidor. Si esto ocurre, no será posible imprimir hasta que la cola libere algunos documentos.

Mejorar la fiabilidad

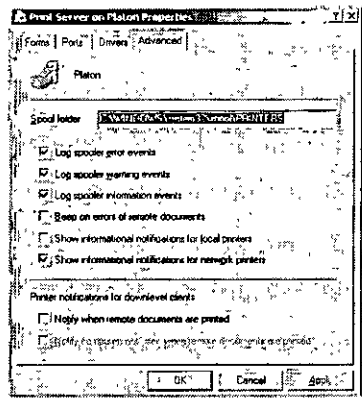
Típicamente, una partición de inicio se encuentra en un disco espejo (RAID 1). Para rendimiento y recuperabilidad, puedes querer mover la cola de impresión a un volumen que tiene RAID 5 y disminuir las probabilidades a un punto simple de fallo del subsistema de un disco.

Para cambiar la ubicación de la carpeta de cola de impresión

1. Abra **Printers and Faxes**.

2. En el menú **File**, haga clic en **Server Properties** y a continuación, haga clic en la pestaña de **Advanced**.

3. En el campo **Spool folder**, escriba la ruta de acceso y el nombre de la nueva carpeta de cola de impresión predeterminada para el servidor de impresión y a continuación, haga clic en **OK**.



4. Detenga y reinicie el servicio de cola de impresión o reinicie el servidor.

Notas

- Si el servidor se utiliza como servidor de impresión para un gran número de impresoras o para trabajos de impresión que suelen ser muy largos, debería mover la carpeta de la cola de impresión a otra ubicación.
- Es posible que la carpeta de cola de impresión requiera una gran cantidad de espacio en disco para poner en la cola de impresión todos los trabajos.
- La carpeta de cola de impresión no debe situarse en el directorio raíz (normalmente C:\).
- Si la carpeta nueva no existe, este procedimiento la crea.

Establecer prioridades de impresión

Puede que quieras configurar prioridades de impresora para dos impresoras que impriman por el mismo dispositivo de impresión. Así podrás garantizar que aquélla que tiene la mayor prioridad imprima por el dispositivo antes que la de baja prioridad. Es una buena estrategia si la impresora con baja prioridad está disponible sólo en horario fuera de oficina y tiene muchos trabajos de impresión en la cola. Si has de imprimir algún trabajo, entonces debes hacerlo seleccionando la de mayor prioridad, en cuyo caso tu trabajo pasará el principio de la cola de impresión.

Veamos ambos puntos iniciales.

Ajusta prioridades entre impresoras para priorizar los documentos que se imprimirán por el mismo dispositivo. Para hacerlo, crea múltiples impresoras señalando al mismo dispositivo de impresión.

Los usuarios pueden enviar documentos críticos a una de mayor prioridad y los que no lo son a una de menor prioridad. Los documentos enviados a la de mayor prioridad se imprimirán primero.

Para ajustar prioridades entre impresoras, efectúa lo siguiente:

- Que dos o más impresoras apunten al mismo dispositivo (mismo puerto). El puerto puede ser cualquier puerto físico del servidor de impresión o un puerto que señale a un dispositivo de impresión con interfaz de red.
- Ajuste diferentes prioridades para cada impresora que esté conectada al dispositivo de impresión y divida a los usuarios en distintos grupos para que impriman en distintas impresoras. También puedes tener usuarios enviando documentos de alta prioridad a la impresora con más alta prioridad y documentos con baja prioridad a la impresora con prioridad más baja.

Cómo usar las prioridades:

Un usuario(1) que envía un trabajo a la impresora con prioridad de '1' y otro usuario(2) que envía un trabajo a una que tiene prioridad '99'. Los documentos del usuario(2) se imprimirán antes que los del usuario(1).

Puedes agilizar la impresión de cualquier documento que ha de imprimirse inmediatamente. Los documentos que se envían con niveles altos de prioridad adelantarán en la cola de impresión a los de baja prioridad que esperan para ser impresos. Si dos impresoras lógicas están asociadas con la misma impresora, Windows Server 2003 ® enviará los documentos con mayor nivel de prioridad en la impresora primero.

Para usar las prioridades, debes crear múltiples impresoras lógicas para la misma impresora física. Luego asigna un nivel de prioridad distinto a cada una de ellas y crea un grupo de usuarios que corresponda igualmente a cada una.

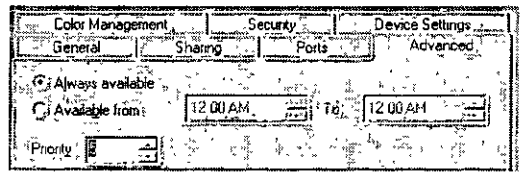
Para establecer prioridades de impresión distintas para grupos diferentes

*1. Abra **Printers and Faxes**.*

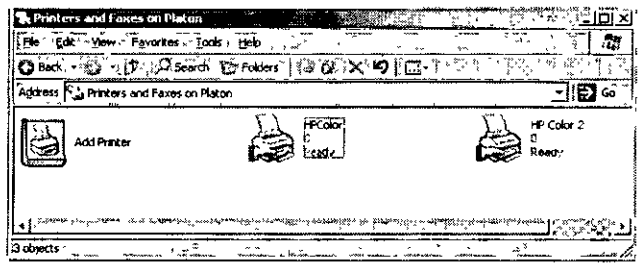
*2. Haga clic con el botón secundario del ratón en la impresora que desee configurar, haga clic en **Properties** y después, haga clic en la pestaña de **Advanced**.*

3. En **Priority**, haga clic en las flechas arriba y abajo y, después, en **OK**.

4. O bien, escriba la prioridad, donde 1 es la prioridad mínima y 99 la máxima, y después haga clic en ***OK****.*



5. Haga clic en ***Add Printer*** *para agregar una segunda impresora lógica para la misma impresora física.*



6. Haga clic en la ficha ***Advanced*** *de* ***Properties*** *de la segunda impresora.*

7. En Prioridad, establezca una prioridad mayor que la que estableció en la primera impresora lógica.

8. Indique al grupo de usuarios normal que utilizará el primer nombre de impresora lógica y al grupo con mayor prioridad que usuará la segunda impresora lógica. Establezca los permisos apropiados para los distintos grupos.

Nota

- *No obtendrá ninguna ventaja si se limita a asignar una prioridad a una impresora. Si desea aprovechar esta opción, debe establecer al menos dos impresoras lógicas distintas para una misma impresora física.*

Programar la disponibilidad de la impresora

Uno de los métodos que permite maximizar el uso de las impresoras consiste en programar horas de impresión alternativas para documentos largos o de tipos determinados. Por ejemplo, si el tráfico de la impresora es intenso durante el día, puede postergar la impresión de los documentos largos y enrutarlos a través de una impresora que únicamente imprima fuera de las horas laborales.

La cola de impresión continúa aceptando documentos, pero no los envía a la impresora de destino hasta la hora de inicio especificada.

En lugar de dedicar un dispositivo de impresión únicamente a la impresión fuera de horas laborables, lo que supone un uso poco eficaz de los recursos, puede asignar distintas impresoras lógicas al mismo dispositivo de impresión y configurar cada una con diferentes horas de disponibilidad. Una impresora podría estar disponible de 6:00 p.m. a 6:00 a.m., mientras que la otra estaría disponible las 24 horas del día. Puede indicar a los usuarios que envíen documentos largos a la impresora disponible sólo fuera de las horas laborables y el resto de los documentos a la impresora que está siempre disponible.

1. Abra ***Printers and Faxes***.

2. Haga clic con el botón secundario del ratón en la impresora que desea establecer y, a continuación, haga clic en **Propierties**.

3. Haga clic en la ficha **Advanced** y a continuación, en **Available from**.

4. Para establecer el período durante el que la impresora estará disponible, realice una de las acciones siguientes:

- Haga clic en la flecha arriba o abajo.
- bien, escriba la hora de inicio y final, por ejemplo **6:00 p.m. a 6:00 a.m.**.

Nota

- De manera predeterminada, las impresoras están siempre disponibles.

Configurar un conjunto de impresoras

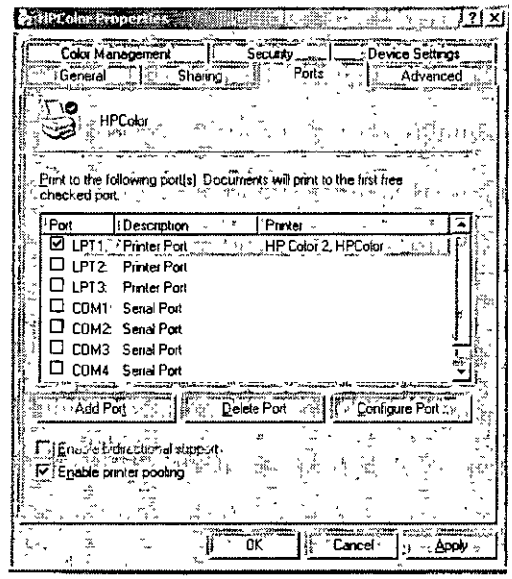
Hemos hablado de configurar varias impresoras lógicas que apunten a un único dispositivo físico, un conjunto de impresoras serían varios dispositivos físicos que se comportan como uno solo, al que se le mandan los trabajos a imprimir y van imprimiéndose en el dispositivo que se encuentre libre o en su caso, añadiéndose a la cola de impresión menos ocupada.

Las impresoras deben ser del mismo tipo y utilizar el mismo controlador de impresión.

1. Abra ***Printers and Faxes.***

2. De clic derecho en la impresora que estamos usando, pulsamos **Properties.**

3. En la ventana de **Properties**, en la pestaña de **Ports**, marcamos la casilla de verificación **Enable printer pooling** (habilitar cola de impresión).



4. Marcaremos cada casilla de verificación por cada puerto que las impresoras que quieras se conecten al conjunto, luego pulsamos en **OK.**

WINDOWS 2003 SERVER®

Tema 8

Implementación de Directiva de Grupos

- El rol de la unidad organizativa
- Modificar permisos para objetos del directorio activo
- Delegar el control de las unidades organizativas

FLORES ALVARES LUIS ARMANDO
GUERRERO MARTÍNEZ EDSON ARMANDO

El rol de la unidad organizativa

Para modelar la estructura social de un sistema de información es importante incluir el concepto de "Rol". Un "Rol" es una abstracción de las actividades, una o más, que una agrupación de usuarios del sistema puede realizar en un instante determinado.

Podemos abordar el problema de la modelización de la estructura social de un sistema desde dos puntos de vista. Por un lado, agrupamos los posibles usuarios del sistema en suborganizaciones dependiendo de las actividades que pueden realizar y fijándonos en aspectos como las restricciones en cuanto al número de miembros de cada una de estas suborganizaciones. En este caso estamos modelando la parte estática de la organización. Por ejemplo, en el caso de un departamento de la Universidad podemos detectar la existencia de distintos subgrupos de los profesores: el del director, el del secretario y el de un conjunto de comisiones encargadas de realizar actividades relacionadas con la gestión.

Desde otro punto de vista necesitamos modelar cómo un usuario puede llegar a formar parte de cada una de dichas suborganizaciones y cómo sus miembros pueden ir evolucionando a lo largo del tiempo (¿puede un profesor llegar a director?) En este caso nos fijamos en los aspectos dinámicos de la organización, en su posible evolución a lo largo de la vida del sistema.

Como ejemplo de suborganizaciones podemos introducir el concepto de grupo (tipo de Unidad Organizativa). Un grupo se define como un conjunto de usuarios que, de forma esporádica, se unen para la realización de una o más actividades. Otro ejemplo nos lo da el concepto de departamento, definido como una división estructural de la organización. Si analizamos los ejemplos anteriores, observamos que existen dos tipos de suborganizaciones: las estáticas, que describen la estructura general de la organización y las dinámicas, que modelan agrupaciones de usuarios que se crean para la realización de una tarea concreta.

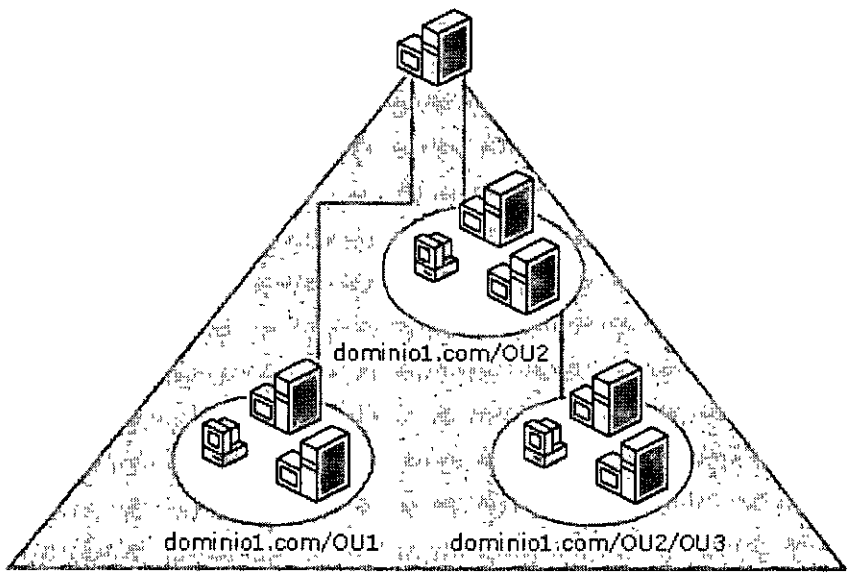
Cada actor, ya sea un usuario o uno de los elementos de la unidad organizativa, desempeña un rol determinado en el sistema en cada instante. El desempeño de un rol implica la posibilidad o capacidad de poder realizar un conjunto de actividades asociadas al mismo.

Por último, podemos observar cómo entre roles (refiriéndonos al conjunto de los actores que están desempeñando el rol en un instante de tiempo) y unidades organizativas se refleja una o más relaciones denominadas dependencias organizativas. Con estas asignaciones se modelan las relaciones del tipo: posibilidad de pasar de un rol a otro, una suborganización puede ser parte de otra suborganización mas general, etc. En resumen, estas dependencias describen las restricciones entre los conjuntos de posibles usuarios del sistema.

La unidad organizativa es un tipo de objeto de directorio muy útil incluido en los dominios.

Las unidades organizativas son contenedores de Active Directory en los que puede colocar usuarios, grupos, equipos y otras unidades organizativas. Una unidad organizativa no puede contener objetos de otros dominios.

Una unidad organizativa es el ámbito o unidad más pequeña a la que se pueden asignar configuraciones de Directiva de grupo o en la que se puede delegar la autoridad administrativa. Con las unidades organizativas, puede crear contenedores dentro de un dominio que representan las estructuras lógicas y jerárquicas existentes dentro de una organización. Esto permite administrar la configuración y el uso de cuentas y recursos, en función de su modelo organizativo.



Como se muestra en la ilustración, las unidades organizativas pueden contener otras unidades organizativas. La jerarquía de contenedores se puede extender tanto como sea necesario para modelar la jerarquía de la organización dentro de un dominio. Las unidades organizativas permiten disminuir el número de dominios necesarios en una red.

Puede utilizar unidades organizativas para crear un modelo administrativo que se puede ampliar a cualquier tamaño. Un usuario puede tener autoridad administrativa para todas las unidades organizativas de un dominio o sólo para una de ellas. El administrador de una unidad organizativa no necesita tener autoridad administrativa sobre cualquier otra unidad organizativa del dominio.

Por tanto, el objetivo de las unidades organizativas es *estructurar* u organizar el conjunto de los objetos del directorio, agrupándolos de forma coherente. En el Directorio Activo, las unidades organizativas permiten:

a. *Conseguir una estructuración lógica* de los objetos del directorio, de acuerdo con la organización de la *empresa* (por departamentos o secciones, sedes, delegaciones geográficas, etc.). Entre otras ventajas, esta organización le permite al administrador del dominio una gestión más lógica de usuarios, grupos, equipos, etc., pero también le permite a cualquier usuario una búsqueda de los objetos más sencilla cuando explora el directorio buscando recursos (por ejemplo, se podría localizar fácilmente las impresoras compartidas del edificio central de la delegación de Alicante).

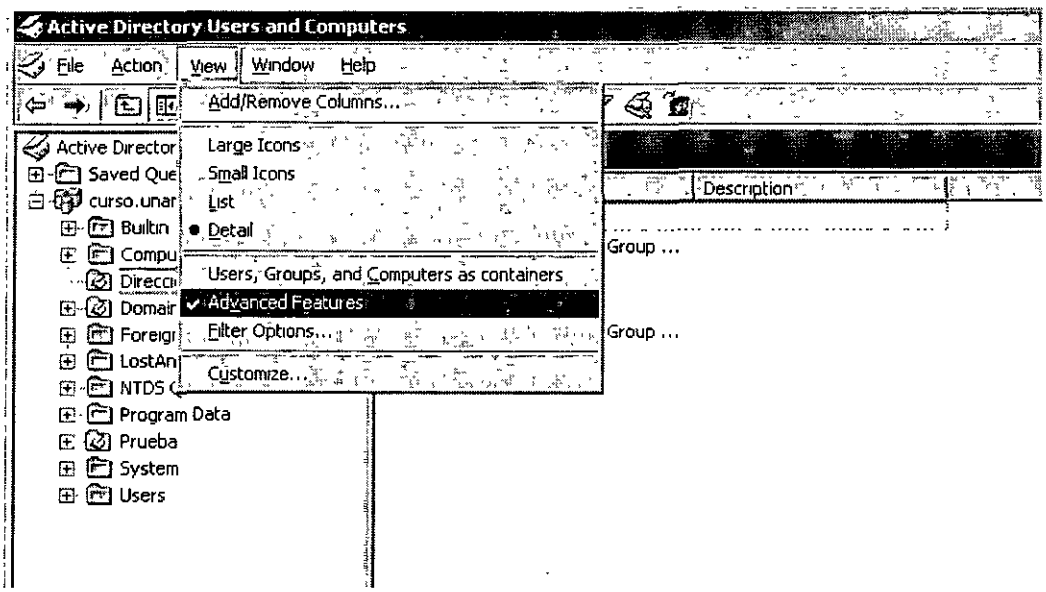
b. *Delegar la administración.* Cada unidad organizativa puede administrarse de forma independiente. En concreto, se puede otorgar la administración total o parcial de una unidad organizativa a un usuario o grupo de usuarios cualquiera. Esto permite *delegar* la administración de subconjuntos estancos del dominio a ciertos usuarios que posean el nivel de responsabilidad adecuada.

c. *Establecer de forma centralizada comportamientos distintos a usuarios y equipos.* A cada unidad organizativa pueden vincularse políticas de grupo, que aplican comportamientos (generalmente en forma de restricciones) a los usuarios y equipos cuyas cuentas se ubican en dicha unidad. De esta forma, podemos aplicar restricciones distintas a subconjuntos de usuarios y equipos del dominio, en función exclusivamente de la unidad organizativa donde se ubican. Por ejemplo, podemos limitar a los usuarios del departamento de contabilidad para que sólo puedan utilizar ciertas aplicaciones, pero que esto no se aplique a los usuarios del departamento de informática.

Modificar permisos para objetos del directorio activo

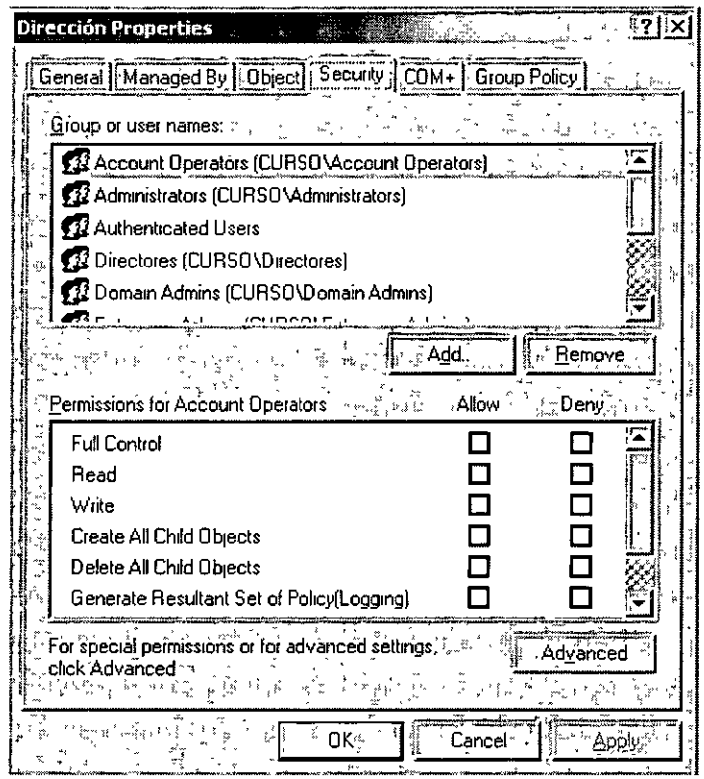
1. Abrir la utilidad de **Active Directory Users and** *Computers* del menú **Administrative Tools** del menú **Start**.

2. Dar clic en el menú **View** y seleccionar la opción **Advanced Features**.



3. Diríjase a la carpeta donde se encuentra el objeto al que desea ver o modificar sus permisos, en el panel derecho se mostrará los objetos que hay dados de alta en esa carpeta en el **Active Directory**.

4. Colocarse sobre el objeto que se desee y dar clic con el botón derecho del ratón para mostrar su menú contextual, seleccionar **Properties**. Seleccionar la ficha **Security**.



5. Si desea configurar los permisos para un nuevo usuario o grupo, haga clic en **Add**. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, escriba el nombre del usuario o del grupo para el que desee configurar los permisos, haga clic en **Chake Names** para comprobar los nombres y después, haga clic en **OK**.

   Podemos dar clic en **Advanced** y luego en **Find Now** para abrir una ventana con todos los posibles usuarios, grupos o equipos a los que se pueden denegar u otorgar permisos.

6. Para conceder o denegar permisos en la lista **Permissions**, haga clic en el usuario o grupo de la lista **Group or user names** y active la casilla de verificación *Allow* o *Deny* situada junto al permiso que desea conceder o denegar

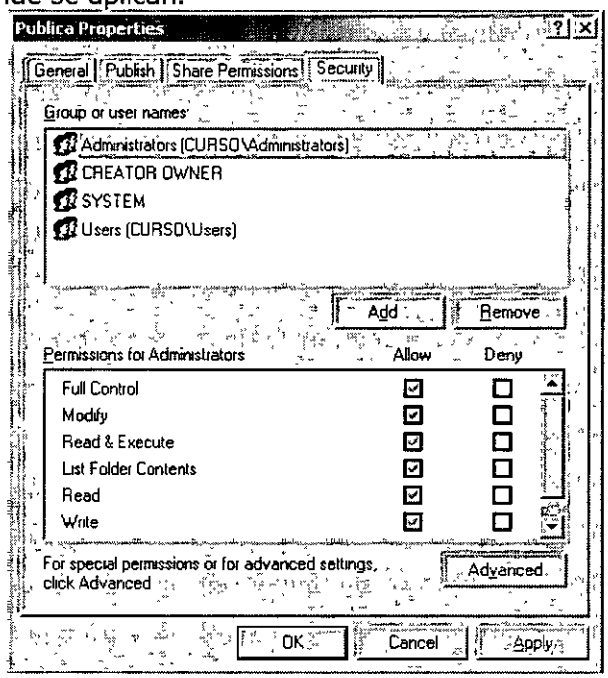
7. O bien, para quitar al grupo o usuario, haga clic en el usuario o grupo de la lista ***Group or user names*** y a continuación, haga clic en **Remove**. Haga clic en **OK**.

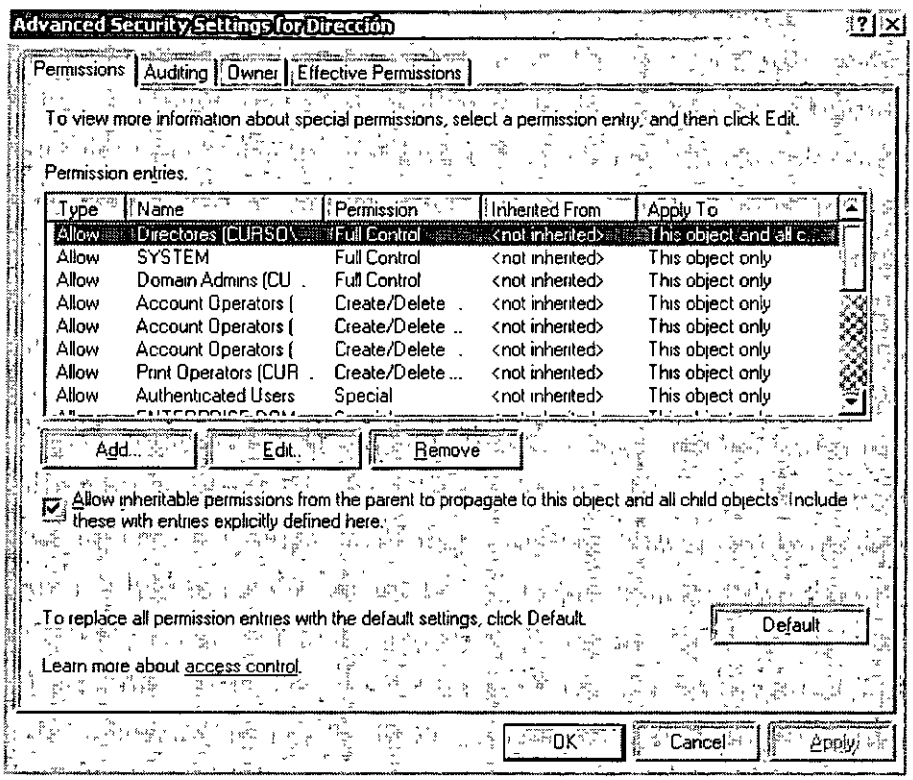
Para configurar, ver, cambiar o quitar permisos especiales:

12. Abrir la utilidad de **Active Directory Users and Computers** del menú ***Administrative Tools*** del menú ***Start***.

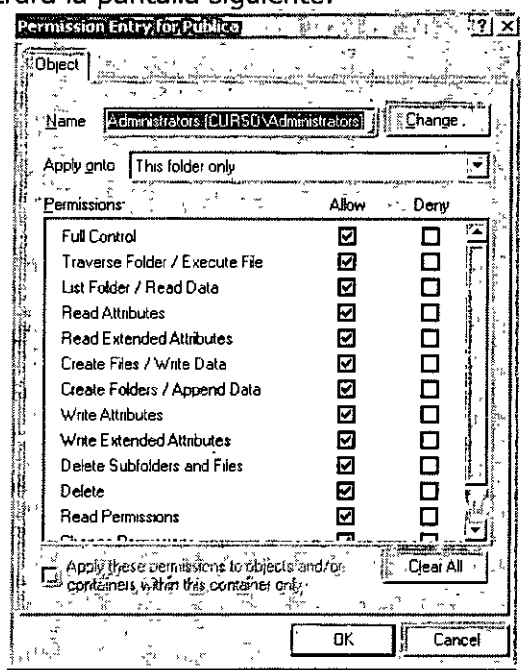
13. Diríjase a la carpeta donde se encuentra el objeto al que desea ver o modificar sus permisos, en el panel derecho se mostrarán los objetos que hay dados de alta en esa carpeta en el Active Directory.

14. Seleccionar la ficha **Security**, marcar en **Advanced**, se mostrará una pantalla en la que se encuentran los nombres de los usuarios, grupos y equipos especiales que tienen permisos sobre dicho directorio o archivo junto con una descripción de los permisos y donde se aplican.





15. Si desea modificar los permisos de alguno de ellos, sitúese sobre él, de clic en **Edit**, y se le mostrara la pantalla siguiente:



En ésta pantalla se muestran los permisos especiales que tiene establecidos el usuario o grupo seleccionado. Si existen casillas en gris, significa que son permisos heredados.

16. Puede modificar los permisos que desee. Para esto, active la casilla correspondiente al permiso deseado en la columna **Allow**, para conceder permisos o **Deny**, para denegarlos.

17. Puede indicar en el apartado ***Apply on to,*** el ámbito de los permisos que está señalado, pudiendo modificar al ámbito desplegando la lista.

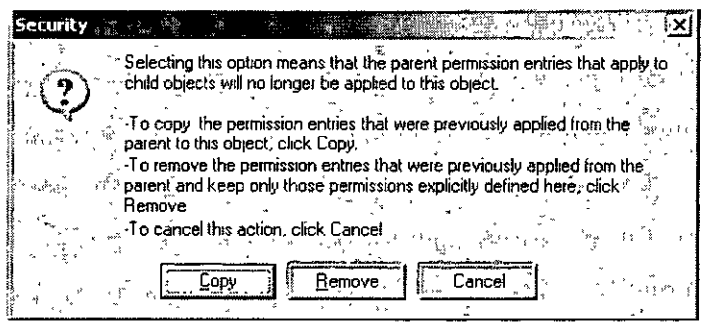
    Si activa **Apply onto this folder only**, evitará que los archivos y subcarpetas secundarias hereden estos permisos. Una vez que haya terminado, dar clic en **OK**.

18. Si se desean añadir otros usuarios o grupos a la lista de nombres, dar clic en *Add*, pulsar en *Advanced* y pulsar en *Fin Now*. Se abrirá una ventana con todos los posibles usuarios, grupos y computadores a las que puede otorgar o denegar permisos.

    Si desea quitar algún usuario o grupo, colóquese sobre él, dar clic en **Remove**.

19. Si quiere que los permisos de la carpeta principal no sean heredados a esta carpeta secundaria, asegúrese que hay casillas de permisos que pueden estar en gris porque son permisos heredados, desactive la casilla **Allow inheritable permissions from the parent to propágate to this object and all child objects...**

    Aparecerá la pantalla siguiente:



- Si se marca la opción **Copy**, concederá al objeto los permisos que tenía el objeto principal y podrán ser modificados.
- Si se marca la opción **Remove**, el objeto no heredará los permisos del objeto principal y podrán añadirse nuevos permisos.

20. Si quiere que los permisos indicados para esta carpeta se hereden a todos los subdirectorios secundarios, active la casilla **Replace permission entries on all child objects with entries shown here that apply to child objects**. Después dar clic en *OK* y se mostrará un cuadro de dialogo que indica que se eliminarán los permisos indicados en los subdirectorios y archivos que cuelgan de este directorio. Dar clic en **Yes** para continuar.

21. Una vez terminados los cambios a los permisos, dar clic en OK para regresar a la pantalla de Propiedades del directorio. Dar clic en OK en la utilidad.

Delegar el control de las unidades organizativas

Si delega la administración, podrá asignar una serie de tareas administrativas a los usuarios o grupos apropiados. Puede asignar tareas administrativas básicas a grupos o usuarios normales y dejar la administración de todo el bosque o de todo el dominio a cargo de los miembros de los grupos Administradores de dominio y Administradores de organización. Al delegar la administración, puede permitir a grupos de su organización ejercer un mayor control sobre los recursos de la red local. También puede ayudar a proteger la red de daños malintencionados o accidentales limitando la pertenencia de los grupos de administradores.

Puede delegar el control administrativo en cualquier nivel de un árbol de dominios mediante la creación de unidades organizativas dentro de un dominio y la delegación del control administrativo de determinadas unidades organizativas a usuarios o grupos específicos.

Para decidir qué unidades organizativas debe crear y cuáles deben contener cuentas o recursos compartidos, tenga en cuenta la estructura de la organización.

Por ejemplo, puede ser aconsejable crear una unidad organizativa que permita conceder a un usuario el control administrativo sobre todas las cuentas de usuario y de equipo en todas las ramas de un departamento, como el de Recursos Humanos. O bien, puede que desee asignar a un usuario el control administrativo de sólo algunos recursos dentro de un departamento; por ejemplo, las cuentas de equipo. Otra delegación posible del control administrativo consistiría en asignar a un usuario el control administrativo de la unidad organizativa Recursos Humanos pero no de otras unidades organizativas incluidas dentro de ella.

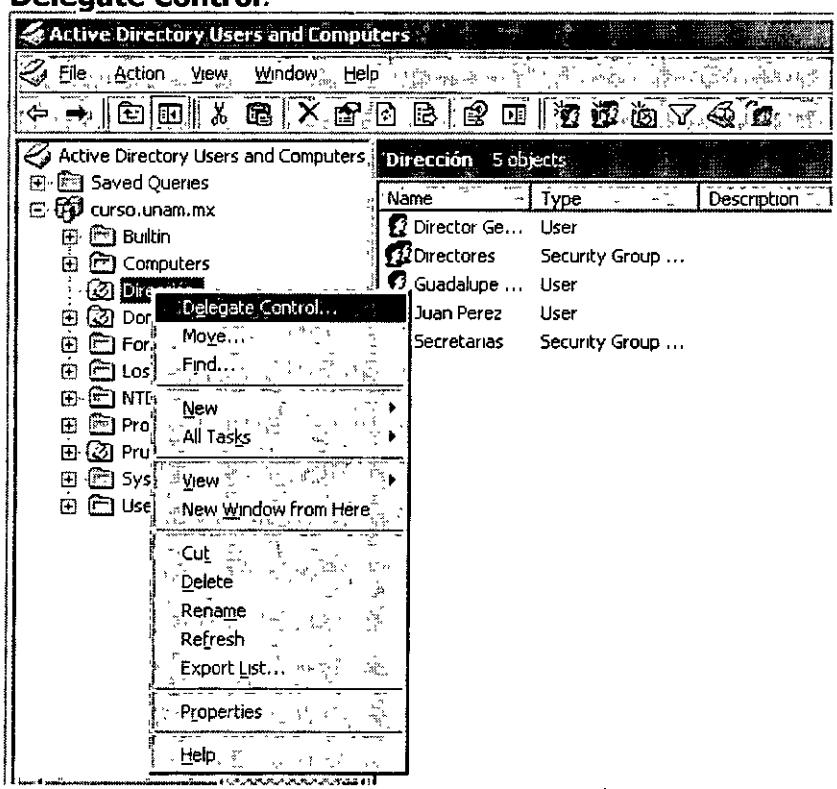
Active Directory define permisos y derechos de usuario específicos que se pueden usar para delegar o limitar el control administrativo. Mediante una combinación de unidades organizativas, grupos y permisos, puede definir el ámbito administrativo más adecuado para una determinada persona, que podría ser un dominio completo, todas las unidades organizativas de un dominio o una sola unidad organizativa.

El control administrativo se puede asignar a un usuario o grupo mediante el uso del Asistente para delegación de control o a través de la consola del Administrador de autorización. Ambas herramientas le permiten asignar derechos o permisos a determinados usuarios o grupos.

Delegar control de una unidad administrativa

1. Abrir la utilidad de **Active Directory Users and Computers** del menú **Administrative Tools** del menú **Start**.

2. Colocarse sobre la unidad organizativa donde desea delegar el control, pulse el botón derecho del ratón para que se muestre su menú contextual, seleccionar **Delegate Control**.

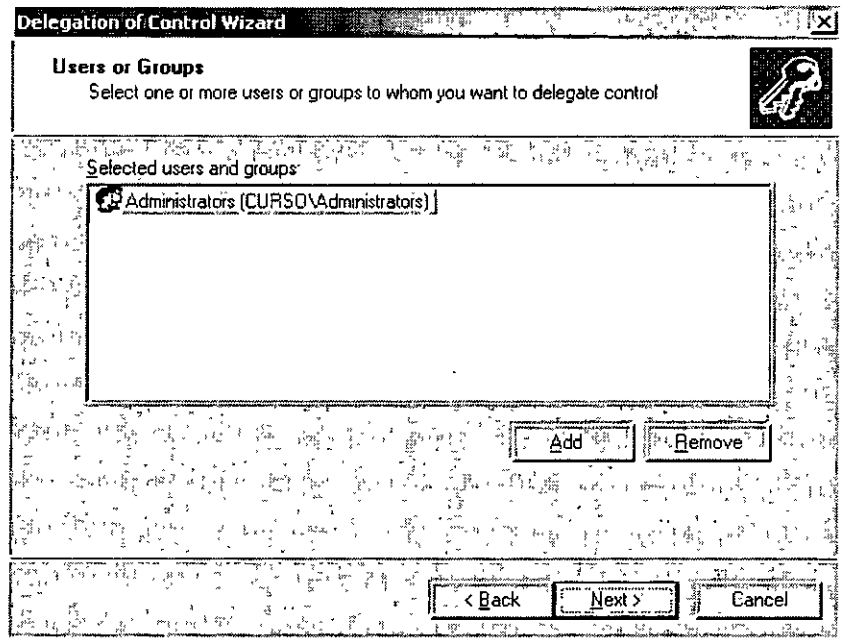


3. Aparecerá el ayudante para la delegación de control. Dar clic en **Next** y aparecerá la ventana de **Users or Groups**.

4. Si desea agregar usuarios o grupos a la lista de nombres, dar clic en **Add**, pulsar en **Advanced**, posteriormente en **Find Now** y se abrirá una ventana con todos los usuarios, grupos, etc. disponibles.

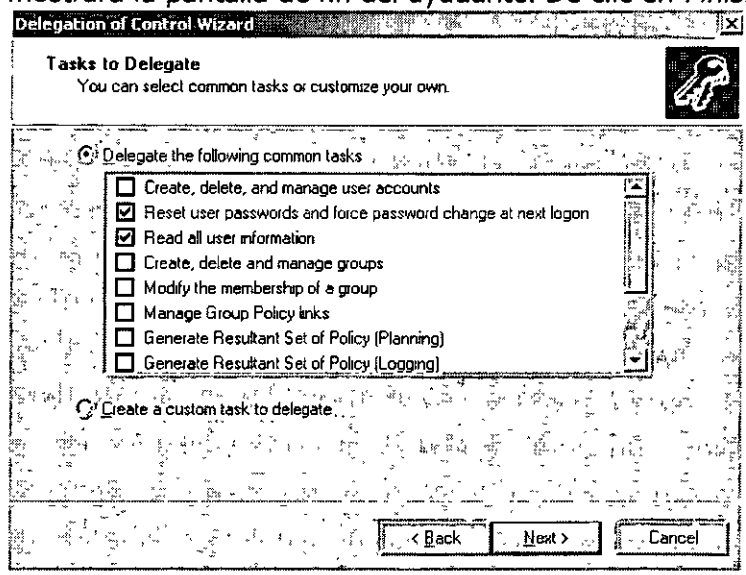
   Seleccione los que desee, y dar clic en OK, de de nuevo clic en OK.

También si quiere quitar algún usuario o grupo, sitúese sobre él y de clic en el botón **Remove**. Una vez finalizadas todas la operaciones de clic en **Next**.

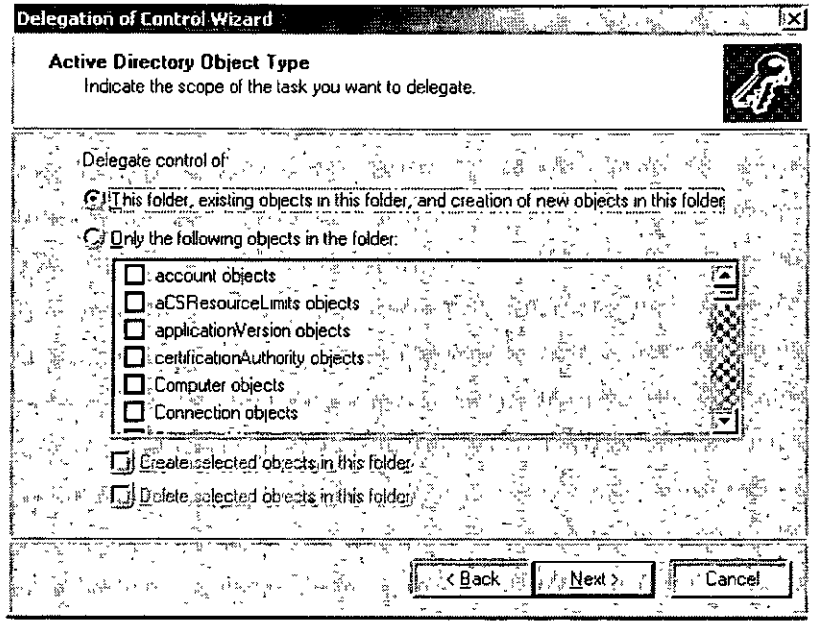


5. Aparecerá la pantalla de **Tasks to Delegate**.

   a. Si quiere delegar todas, o algunas de las tareas más comunes, active las casillas correspondientes. Una vez finalizados los cambios de clic en el botón *Next* y se mostrara la pantalla de fin del ayudante. De clic en *Finish.*



b. Si quiere crear una tarea personalizada que no se encuentre en la lista superior, active la casilla **Create a custom task to delegate**, de clic en **Next** y se mostrara la siguiente pantalla:



En ésta pantalla puede seleccionar delegar el control de esta carpeta con todos los objetos existentes y la creación de nuevos objetos en ella (*This folder, existing objects in this folder, and creation of new objects in the folder*) o solo delegar el control de los objetos deseados (*Only the following objects in the folder*), en este último caso, se deberá indicar los objetos deseados.

Una vez finalizadas las acciones correspondientes dar clic en **Next**.

6. Aparecerá la pantalla de *Permissions* en donde deberá Indicar los permisos que se desean mostrar al usuario o grupo de que esta delegando el control de los objetos seleccionados para que dicho usuario puede permitirlos o denegarlos, y los permisos que le delega sobre dichos objetos.

   Una vez finalizadas las acciones correspondientes dar clic en **Next**. Se mostrará la pantalla final del ayudante, de clic en **Finish**.

7. Para poder ver los permisos que se acaban de dar al usuario o grupo en que ha delegado el control sobre la unidad organizativa, seleccione el contenedor, pulse el botón derecho del ratón para que se muestre su menú contextual, seleccione **Properties**, seleccionar la ficha Security, dar clic en **Advanced** y se mostrará la lista con permisos especiales.

WINDOWS 2003 SERVER

Tema 9

Implementación de Directiva de Grupos

- Implementar objetos de directiva de grupos
- Implementar objetos de directiva de grupos en un dominio
- Administrar la implementación de una directiva de grupos

FLORES ALVARES LUIS ARMANDO
GUERRERO MARTINEZ EDSON ARMANDO

Implementar objetos de directiva de grupos

¿Qué es Group Policy?

Las Directivas de Grupo son colecciones de configuraciones de usuarios y computadoras. Group Policy le otorga control de administración sobre los usuarios y las computadoras de una red Windows, y por lo tanto le permite definir el estado del ambiente de trabajo de los usuarios una sola vez. También se puede aplicar configuraciones de Group Policy a través de una organización entera o a grupos específicos de usuarios y de computadoras.

¿Qué es una directiva de grupo?

Un objeto de directiva de grupo (GPO: Group Policy Object) es un conjunto de una o más políticas del sistema. Cada una de las políticas del sistema establece una configuración del objeto al que afecta. Por ejemplo, tenemos políticas para:

Ocultar el panel de control
Deshabilitar el uso de REGEDIT.EXE y REGEDT32.EXE
No permitir el uso del cmd

Directivas según su función

Hay dos tipos troncales de directivas según su función:

1. **Directivas de seguridad**: ¿Cuántos caracteres tiene una contraseña? ¿Cada cuanto tiempo debe ser cambiada ésta?, etc. Pueden ser aplicadas:

   a. ***A nivel de dominio***: Son aplicadas en todas las máquinas del dominio.

   b. ***A nivel de controladores de dominio***: Se aplican tan sólo en los controladores de dominio, pero sin suplantar a las del dominio (en caso de entrar en contradicción una y otra, se aplica la del dominio, no la de los controladores de dominio).

2. **Directivas de Entorno (GPO - Group Policy Object)**: ¿Quién tiene acceso al panel de control? ¿Cuál es el tamaño máximo del archivo de registro de sistema? Pueden ser aplicadas:

a. A nivel de equipo local
b. A nivel de sitio
c. A nivel de dominio
d. A nivel de Unidad Organizativa (OU -> Organizational Unit).

Directivas según el objeto al que configuran

Respecto al objeto al que configuran también son dos:

e. Configuración del equipo: que se divide en:

i. Configuración de software
ii. Configuración de Windows
iii. Plantillas administrativas

f. Configuración del usuario que se dividen igual que la anterior.

Las GPO's pueden estar contenidas en varios tipos de objetos:

1. **Equipos Locales**: son aplicadas únicamente en el equipo que las tiene asignadas independientemente del dominio al que pertenezcan. Estas son las únicas políticas que se aplican a los equipos que no están en un dominio, como servidores independientes.

2. **Sitios de Active Directory**: se aplican para todos los equipos y/o usuarios de un sitio, independientemente del dominio del mismo bosque al que pertenezcan.

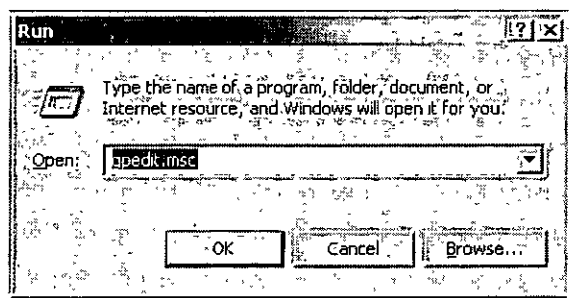
3. **Dominios de Active Directory**: se aplican a todos los equipos y/o usuarios de un dominio.

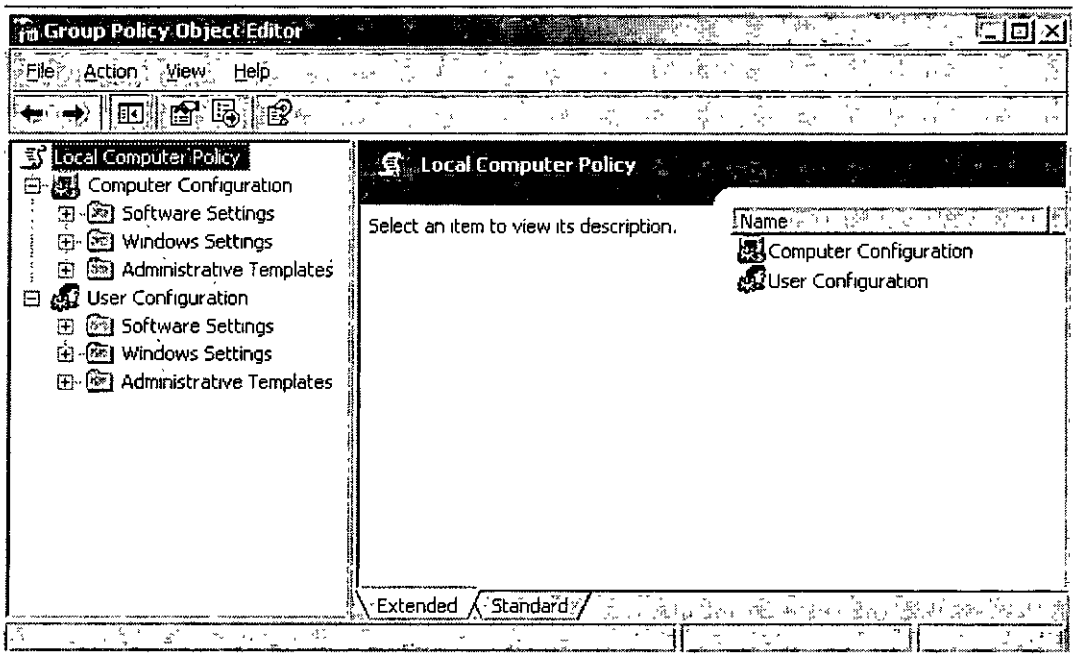
4. **Unidades Organizativas de Active Directory**: se aplican únicamente a los equipos y/o usuarios que pertenezcan a una unidad organizativa (OU).

Crear una nueva directiva de grupo

1. Dar clic en la opción *Run* del menú *Start.*

2. Escribir gpedit.msc para abrir la utilidad de *Group Policy Object Editor.*

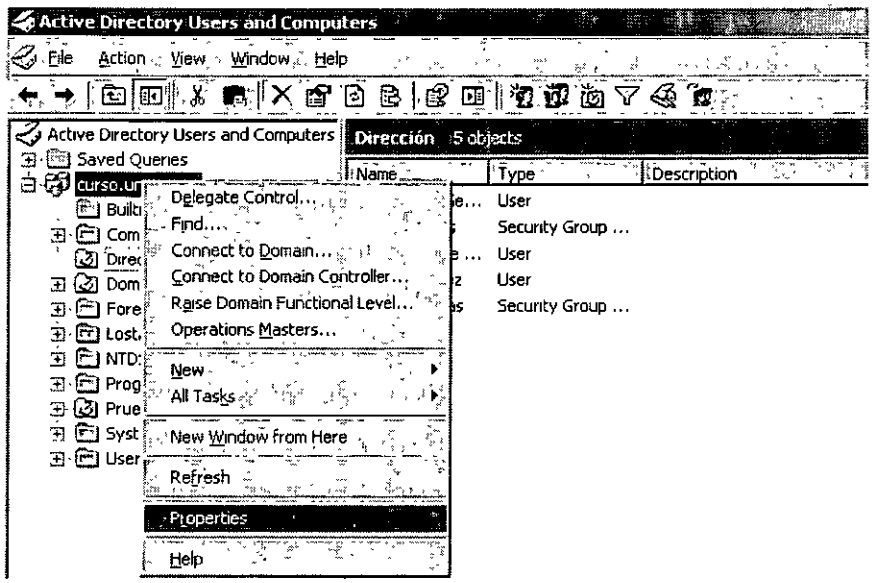




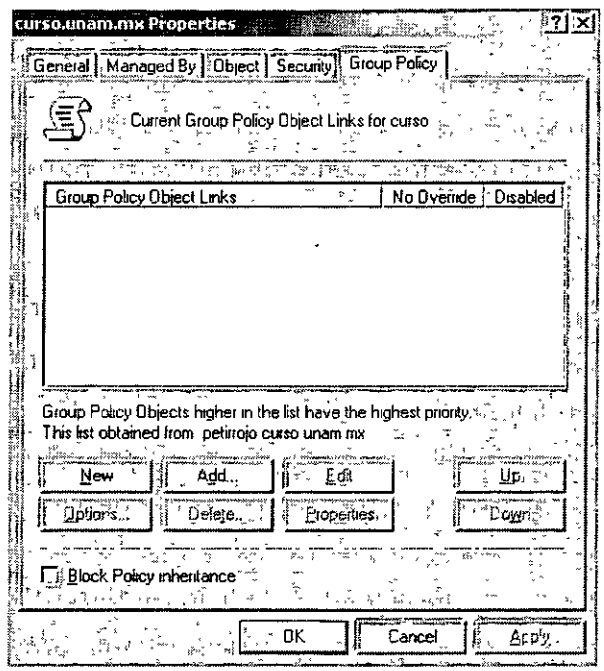
Implementar objetos de directiva de grupos en un dominio

1. Abrir la utilidad de *Active Directory Users and Computers* del menú *Administrative Tools* del menú *Start*

2. Colóquese sobre el dominio o la unidad organizativa donde va a crear la directiva de grupo, de clic con el botón derecho del ratón para que muestre su menú contextual, seleccione la opción *Properties.*

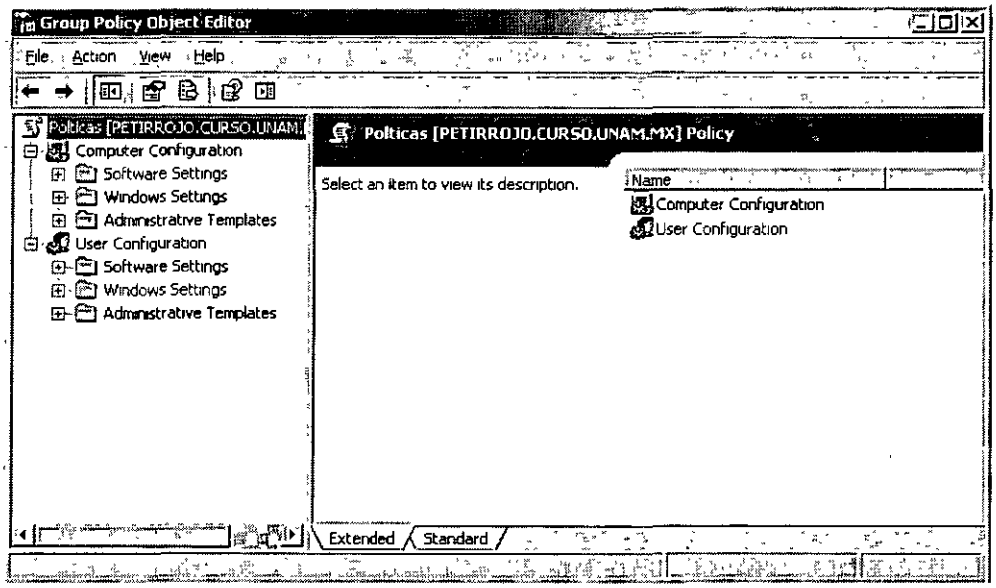


3. Aparecerá la venta de las propiedades del dominio, en donde hay que seleccionar la ficha *Grouo policy*



4. Dar clic en New, indicar el nombre que desea dar y pulse Enter.

5. Si quiere establecer los valores que desee, colóquese sobre la directiva de grupo que acaba de crear, dar clic en el botón *Edit y se muestra la siguiente ventana*



6. Hacer las modificaciones que considere oportunas a lo largo de los apartados disponibles de las distintas opciones.

Administrar la implementación de una directiva de grupos

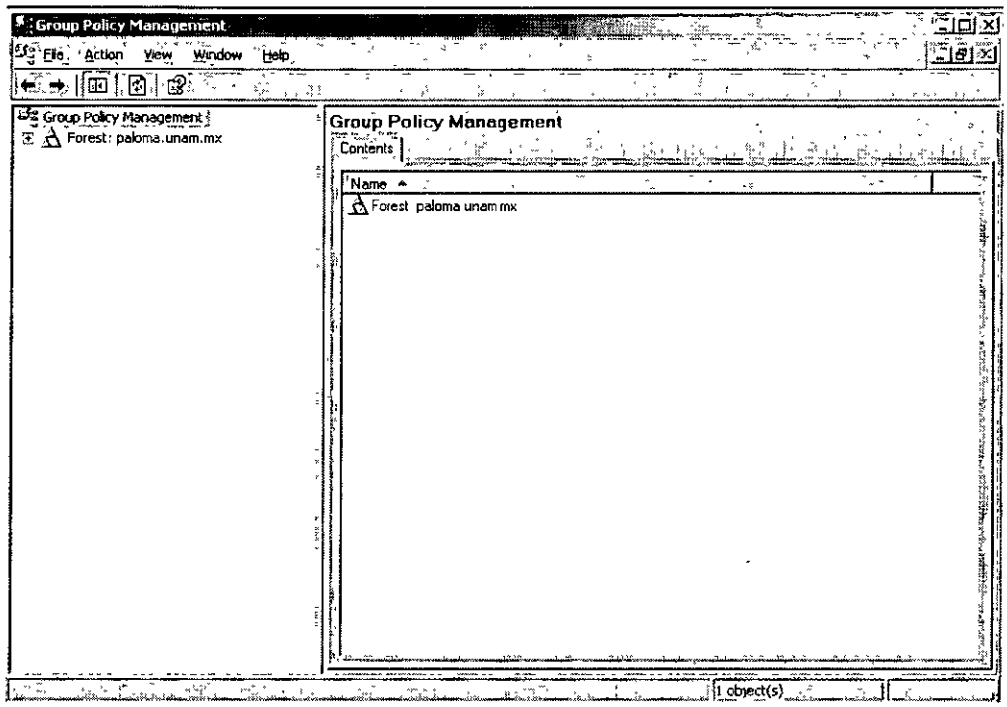
Existe una consola de administración de directiva de grupo (GPMC) es una nueva herramienta para la administración de Directivas de grupo que ayuda a los administradores a administrar una empresa de forma más rentable al mejorar la capacidad de administración y aumentar la productividad

GPMC simplifica la administración de la Directivas de grupo al proporcionar un único lugar para administrar aspectos esenciales de la Directiva de grup

1. Descargar el archivo gpmc.msi.

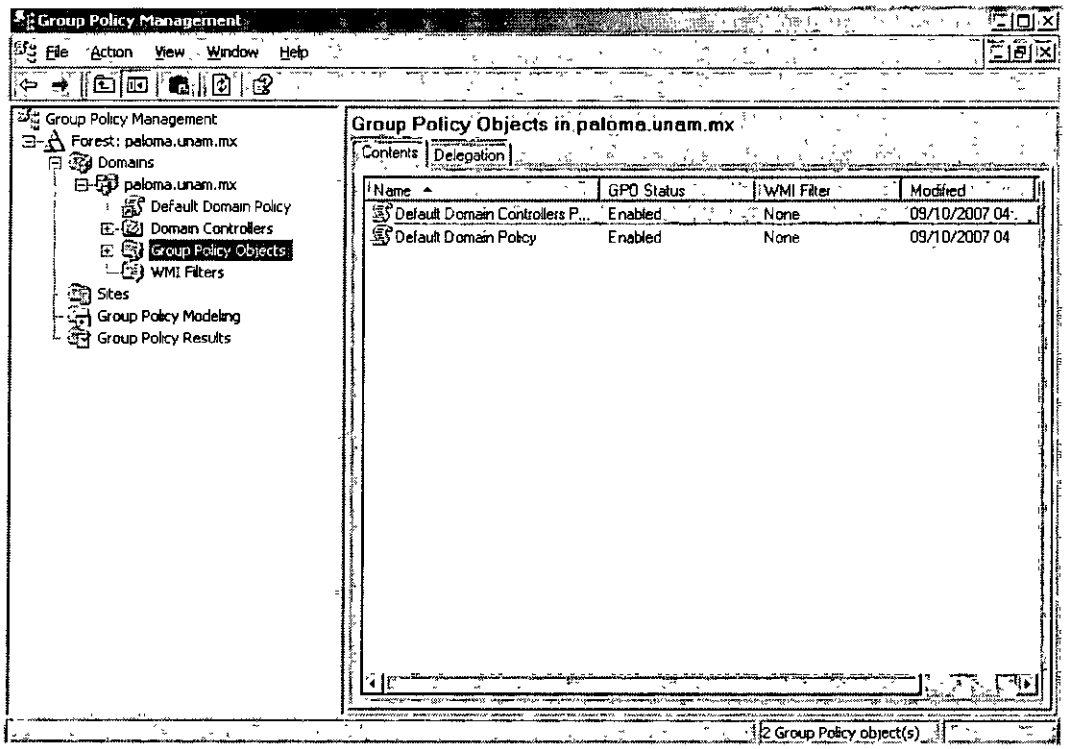
2. Una vez descargada, hacer doble clic sobre el archivo descargado y seguir los pasos pertinentes para instalar la aplicación.

3. Haga clic en el botón *Start*, en *Run*, escriba gpmc.msc y, a continuación, haga clic en Aceptar, se mostrara la pantalla de *Group Policy Management*.



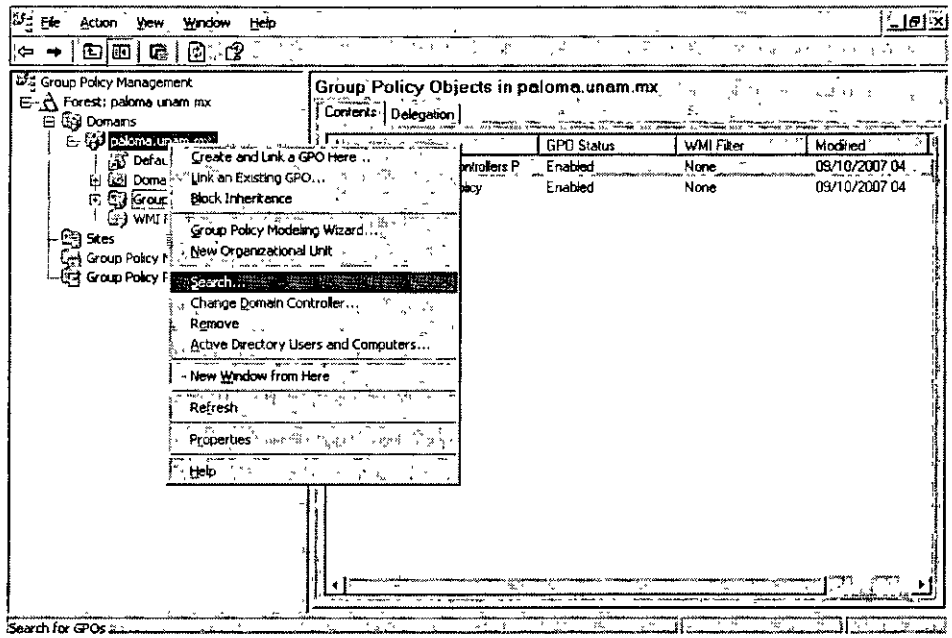
4. Para ver objetos de Directiva de grupo asociados a un contenedor determinado

   En el árbol **Dominios**, haga clic en el árbol. Los objetos de Directiva de grupo asociados al contenedor (la raíz del dominio) aparecen como se muestra en la Figura siguiente. Este concepto se puede aplicar a cualquier contenedor de dominio.

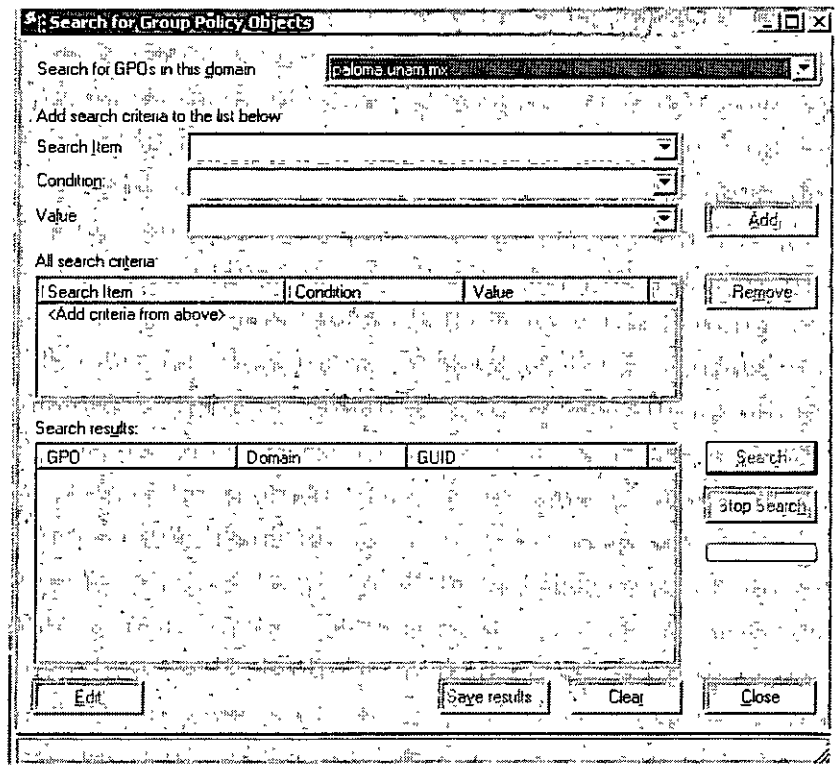


Para buscar un objeto de Directiva de grupo específico en el bosque contoso.com mediante varios parámetros de búsqueda

1. En el árbol de la consola haga clic con el botón derecho del raton en el dominio y continuación haga clic en *Search.*



2. En el cuadro **Search Item** , seleccione un valor dependiendo de la búsqueda deseada, seleccione un valor para **Value**, a continuación, haga clic en **Add**.



3. Haga clic en **Search**. Esto buscara el objeto de directiva con los valores ingresados.

WINDOWS 2003 SERVER ®

Tema 10

Administración del Entorno de Usuario utilizando una Directiva de Grupos

- Configurar opciones de la directiva de grupos
- Asignar Scripts con la directiva de grupos
- Configurar la redirección de carpetas
- Determinar los GPO (objetos de la directiva de grupo) aplicados
- Consejos prácticos para administrar grupos

FLORES ALVARES LUIS ARMANDO
GUERRERO MARTÍNEZ EDSON ARMANDO

En general, las Directivas de Grupo son pasadas hacia abajo desde contenedores padre a contenedores hijo. Si se tienen asignadas Directivas de Grupo por separado en un contenedor padre, esas directivas son aplicadas a todos los contenedores bajo el contenedor padre, incluyendo los usuarios y computadoras del mismo. Sin embargo, si se define una Directiva de Grupo para un contenedor hijo, la directiva del contenedor hijo anula la configuración de directiva heredada desde el padre.

Si una OU tiene directivas que no están configuradas, la OU hija no las hereda. Las directivas que están deshabilitadas son heredadas como deshabilitadas. También, si una directiva es configurada en una OU padre, y la misma directiva no es configurada en la OU hija, la hija hereda las directivas padre.

Si una directiva padre y una directiva hija son compatibles, la hija hereda la directiva padre y la configuración de la hija también se aplica.

Si una directiva configurada para una OU padre es incompatible con la misma directiva configurada en una OU hija, la hija no hereda la directiva del padre y la configuración de la hija es aplicada.

¿Qué es gpupdate?

Es una herramienta command-line que actualiza los local Group Policy settings y Group Policy settings almacenados en Active Directory, incluidas las configuraciones de seguridad. Por defecto, las configuraciones de seguridad se actualizan cada 90 minutos en un puesto de trabajo o un servidor, y cada cinco minutos en un Domain Controller. Usted puede correr gpupdate para probar una Group Policy setting o aplicar inmediatamente un Group Policy setting.

```
gpupdate [/Target:{Computer | User}] [/Force]
[/Wait:Value] [/Logoff] [/Boot] [/Sync]
```

¿Qué es gpresult?

Group Policy genera un reporte que resulta de aplicar políticas al logon. ***Gpresult*** exhibe el reporte que resulta de aplicar políticas que se hacen cumplir en la computadora para el usuario especificado al logon.
El comando ***gpresult*** exhibe los Group Policy settings y el Resultant Set of Policy (RSoP) para un usuario o una computadora. Usted puede utilizar ***gpresult*** para ver qué configuraciones de la GPO son efectivas y localizar problemas en la aplicación.

```
gpresult [/s Computer [/u Domain\User /p Password]]
[/user TargetUserName] [/scope {user|computer}] [/v]
[/z]
```

Asignar scripts con directivas de grupo

Podemos utilizar las directivas para implantar scripts a los usuarios y equipos. Un script es un archivo de lotes o un vbs (Visual Basic Script) que puede ejecutar código o llevar a cabo tareas de administración. Podemos usar los valores de script de las directivas para automatizar el proceso de ejecución de scripts.

Hay valores de script bajo ambas configuraciones, de equipo y de usuario, de la directiva. Podemos usar una directiva para ejecutar un script cuando se inicia o apaga un equipo y cuando un usuario inicia o cierra sesión. Como con todos los valores de directiva podemos configurar el script en la directiva una vez y Windows Server 2003 aplicarlo e implementarlo continuamente por toda tu red.

¿Cuales son los valores de script de directiva?

Estos valores podemos usarlos para centralizar la configuración de los scripts y ejecutarlos en las situaciones mencionadas. Podemos especificar cualquier script que funcione en Windows Server 2003, archivo de lotes, ejecutables y cualesquiera script compatible por Windows Script Host (WSH).

Para ayudarnos a administrar y configurar el entorno de los usuarios, podemos:

- Ejecutar scripts que lleven a cabo tareas que no podemos hacer por medio de otros valores de directiva. Por ejemplo, entorno de usuario con conexiones de red, conexiones de impresoras, accesos directos a aplicaciones y documentos corporativos.
- Limpiar los escritorios cuando los usuarios cierran sesión o apagan el equipo. Podemos quitar conexiones que se hayan añadido con otros scripts de inicio y dejar el equipo en el mismo estado antes de que iniciase sesión el usuario.
- Ejecutar scripts ya existentes para gestión del entorno de usuarios hasta que configuremos otros valores de directiva que los remplacen.

Nota: Desde **usuarios y equipos de Active Directory**, podemos asignar scripts de inicio de sesión individualmente a cuentas de usuario en el cuadro de diálogo de propiedades para cada cuenta. Sin embargo, implantarlos con directivas es preferible para la ejecución de scripts, porque podemos administrarlos de forma centralizada, junto al inicio, apagado, y cierre de sesión.

La sección *Scripts* permite especificar dos tipos de scripts:

- **Starup/Shutdown (Encendido/Apagado).** Se ejecutan cuando la computadora es encendida o apagada.
-

- **Inicio de Sesión/Cierre de Sesión (Logon/Logoff).** Se ejecutan cuando un usuario se autentifica o cierra su sesión de la computadora.

Cuando se asignan múltiples scripts, Windows 2000/2003 ejecuta dichos scripts de arriba hacia abajo. Se puede determinar el orden de ejecución desde el cuadro de dialogo **Properties**.

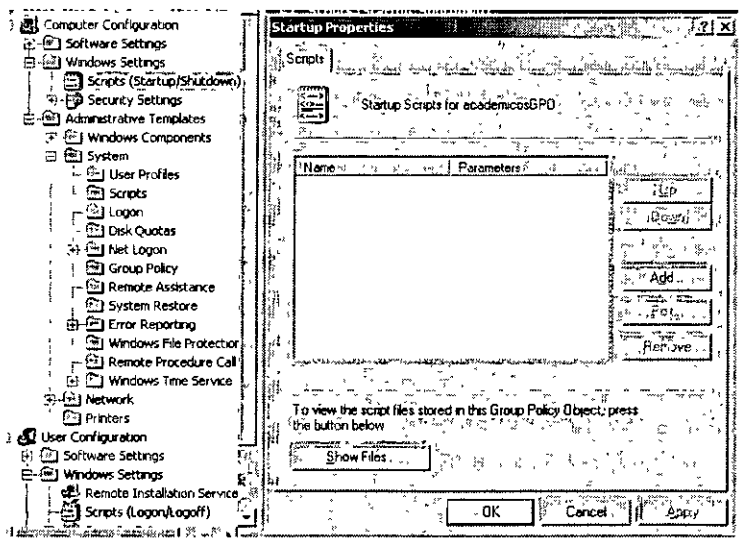
Los administradores pueden usar cualquier lenguaje de scripts compatible con ActiveX. Algunos de los cuales incluyen VBScripts, JScript, Perl y archivos de proceso por lotes de MS-DOS (.bat y .cmd)

La sección de *Configuraciones de Seguridad* permite configurar los niveles de seguridad asignados a un GPO local o no local.

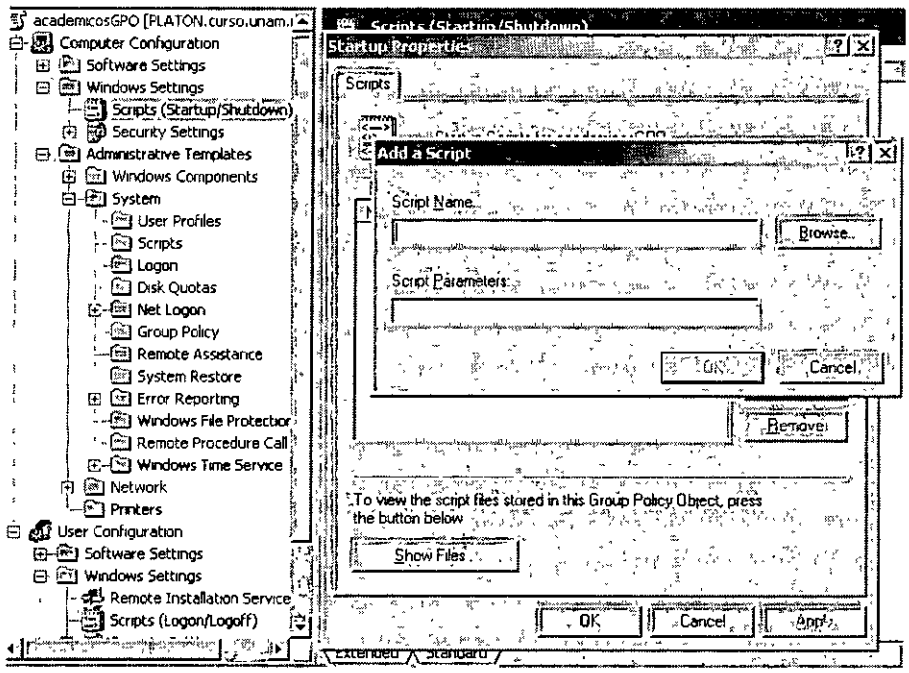
La Configuración de Windows contiene directivas adicionales en la sección de Configuración de Usuario, estas son: *Mantenimiento de Internet Explorer, Servicios de Instalación Remota (RIS) y Redirección de Directorios.*

Una vez que se ha escrito el archivo o secuencia de comandos que se desea ejecutar y se haya indicado que se utilice, vaya a la directiva de grupo correspondiente y siga los siguientes pasos:

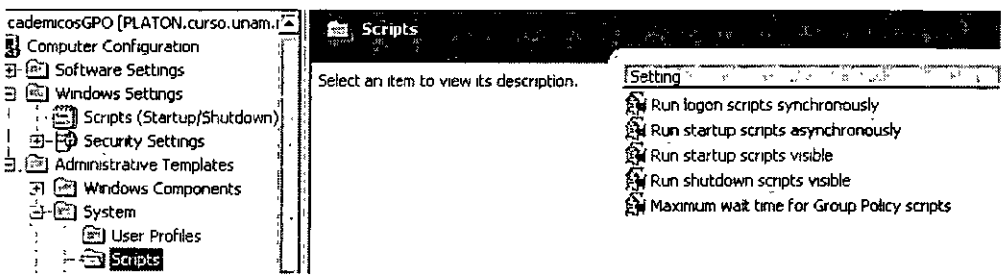
1. Sitúese en el apartado Scripts(Logon/Logoff) de Windows Settings correspondiente al usuario o en el aparatado de Scripts (Shutdown/Startup) de Windows Settings correspondiente al equipo, pulse botón izquierdo del ratón y le mostrara en el panel derecho las opciones correspondientes.



2. Pulse dos veces el botón izquierdo del Mouse sobre la opción correspondiente del panel derecho donde se desea que se ejecute el archivo de comandos que se ha preparado.
3. Marque en add, indique el nombre del archivo de comandos que desea ejecutar (si no lo sabe pulse sobre browse y búsquelo), los parámetros que desee para el archivo (si necesita alguno), marque en OK y pasara a la pantalla de Properties correspondiente. Si hay mas de un archivo de comandos a ejecutar, pude indicar el orden que se desea pulsando arriba o abajo.



4. Cuando haya finalizado, marque en aceptar y volverá a la pantalla de configuración de la directiva de grupo correspondiente.



Ahora hay varias directivas que se pueden configurar para definir mejor la ejecución de los archivos de comandos. Para hacerlo siga los siguientes pasos:

a) Sitúese en el nodo de Scripts de la parte de System en Administrtative Templates correspondientes al usuario o al equipo, pulse el botón izquierdo del ratón y le mostrara en el papel derecho las directivas correspondientes.
b) Hay varias directivas que permiten habilitar la ejecución de los archivos de forma síncrona, se ejecutan antes de cargar el Explorador de Windows y crear el escritorio o asíncrona, se ejecutan simultáneamente a la carga del Explorador de Windows y crear el escritorio; visible muestran instrucciones de los archivos de comandos mientras se ejecutan o invisible, no muestran las instrucciones de los archivos de comandos mientras se ejecutan, y el tiempo de espera máximo para las secuencias de comandos, que determinan cuanto espera el sistema hasta que se ejecuten las secuencias de comandos.
c) En cada uno de los casos deberá indicar, como mínimo si esta habilitada (se aplica), deshabilitada (no se aplica) o si no se ha configurado y marcan en OK para volver a la pantalla de configuración de la directiva de grupo correspondiente.

Configurar la redirección de carpetas

En el Editor de objetos de directiva de grupo, puede utilizar Redirección de carpetas para redirigir determinadas carpetas especiales a ubicaciones de red. Las carpetas especiales son aquellas carpetas, como Mis documentos y Mis imágenes, que se encuentran en Documentos y Configuración. Redirección de carpetas se encuentra en Configuración de usuario, en el árbol de consola del Editor de objetos de directiva de grupo.

Hay varias opciones básicas para la redirección de carpetas. Para cada opción básica existe una versión avanzada. La versión avanzada proporciona mayor control al permitir la redirección basada en la pertenencia a los grupos de seguridad.

Carpeta especial	Notas
Datos de programa	Una configuración de Directiva de grupo controla el comportamiento de Datos de programa cuando está habilitada la caché del cliente. Busque en Configuración de usuario\Plantillas administrativas\Red\Archivos sin conexión en el árbol de consola del Editor de objetos de directiva de grupo.
Escritorio	El escritorio se puede redirigir independientemente de las demás carpetas especiales.
Mis documentos	Mis documentos es la ubicación predeterminada en el shell para que los usuarios guarden sus documentos e imágenes.

Carpeta especial	Notas
Mis documentos\Mis imágenes	Mis imágenes se puede redirigir independientemente de Mis documentos o se puede hacer que siga a Mis documentos (para que sus subcarpetas permanezcan cuando Mis documentos se redirija), tal como está configurado de forma predeterminada. Se recomienda el comportamiento predeterminado a menos que se tenga un motivo específico (como la escalabilidad del servidor) para separar Mis imágenes de Mis documentos. Si estas carpetas se separan, un acceso directo ocupa el lugar de la carpeta Mis imágenes en Mis documentos.
Menú Inicio	Cuando el menú Inicio se redirige, sus subcarpetas siempre lo siguen.

Precaución

Al crear un directorio de redirección de carpetas compartidas, limite el acceso a sólo aquellos usuarios que lo necesitan. Las carpetas redirigidas pueden contener información personal como documentos confidenciales y certificados EFS; se debe procurar proteger el acceso a la carpeta compartida. Restrinja el acceso a la carpeta compartida a sólo aquellos usuarios que lo necesitan. También puede crear un grupo de seguridad de usuarios que requieren permisos para una carpeta compartida determinada y limitar el acceso a únicamente esos usuarios.

Cuando cree la carpeta compartida, ocúltela colocando el símbolo **$** después de su nombre. De esta forma, la carpeta compartida se oculta a los exploradores ocasionales y no aparecerá en Mis sitios de red.

Ventajas de la redirección de Mis documentos

Algunas de las siguientes ventajas afectan a la redirección de cualquier carpeta, pero la redirección de Mis documentos puede ser particularmente beneficiosa dado que esta carpeta tiende a agrandarse con el tiempo.

Cuando se utilizan los perfiles de usuario móviles, sólo la ruta de acceso de red de la carpeta Mis documentos es parte del perfil, no la carpeta Mis documentos. Por tanto, el contenido no tiene que copiarse entre el equipo cliente y el servidor cada vez que el usuario inicia o cierra una sesión, y este proceso puede resultar más rápido de lo que era en Windows NT 4.0.

Incluso si un usuario inicia una sesión en varios equipos de la red, los documentos siempre están disponibles.

La tecnología Archivos sin conexión hace posible que los usuarios tengan acceso a Mis documentos incluso si no están conectados a la red. Esta característica es particularmente útil para los usuarios que utilizan equipos portátiles.

Se puede realizar una copia de seguridad de los datos almacenados en una carpeta de red compartida como parte de la administración rutinaria del sistema. Esto es más seguro, ya que no se requiere ninguna acción por parte del usuario.

Como administrador, puede utilizar la Directiva de grupo para establecer cuotas de disco, con lo que limita la cantidad de espacio que ocupan las carpetas especiales de los usuarios.

Los datos que son específicos de un usuario pueden redirigirse a otro disco duro del equipo local del usuario desde el disco duro en el que se encuentran los archivos del sistema operativo. Así, los datos del usuario estarán más seguros si tiene que volver a instalar el sistema operativo.

Permitir derechos exclusivos en carpetas especiales

La ficha **Configuración**, en el cuadro de diálogo de propiedades de cada carpeta, contiene una casilla de verificación llamada **Permitir al usuario derechos exclusivos en Mis documentos**. Si activa esta casilla de verificación, solamente el usuario y el sistema local tendrán control total sobre la carpeta, por lo que ni siquiera el administrador tiene derechos sobre la misma. Si desactiva esta casilla de verificación, no se realiza ningún cambio en los permisos de la carpeta. Los permisos que se apliquen siguen teniendo efecto de manera predeterminada.

Consideraciones acerca de la eliminación de directivas con respecto a Redirección de carpetas

La tabla siguiente resume lo que sucede cuando el objeto de directiva de grupo deja de aplicarse a las carpetas redirigidas y a su contenido.

Valor Mover el contenido de la carpeta especial a la nueva ubicación	Opción Eliminación de la directiva	Resultados cuando se quita la directiva

Habilitado	Devolver la carpeta a la ubicación local de perfil de usuario cuando la directiva se haya quitado	La carpeta especial vuelve a la ubicación del perfil de usuario. El contenido se copia de nuevo, no se mueve, a la ubicación del perfil de usuario. El contenido no se elimina de la ubicación redirigida. El usuario todavía tiene acceso al contenido, pero sólo en el equipo local.
Deshabilitado	Devolver la carpeta a la ubicación local de perfil de usuario cuando la directiva se haya quitado	La carpeta especial vuelve a la ubicación del perfil de usuario. El contenido no se copia ni se mueve a la ubicación del perfil de usuario. Precaución Si el contenido de una carpeta no se copia en la ubicación del perfil de usuario, el usuario no puede verlo
Habilitado o Deshabilitado	Cuando se quite la directiva, dejar la carpeta en la nueva ubicación	La carpeta especial permanece en la ubicación redirigida. El contenido permanece en la ubicación redirigida. El usuario sigue teniendo acceso al contenido de la carpeta redirigida.

Redirección de carpetas y Archivos sin conexión

La tecnología Archivos sin conexión se aplica a las unidades montadas o asignadas que contienen documentos o datos que tal vez el usuario desee utilizar sin conexión. Archivos sin conexión no depende de Redirección de carpetas. Se instala y configura en servidores de red compartidos independientemente del complemento Redirección de carpetas. Archivos sin conexión permite al usuario trabajar eficazmente aunque no esté conectado a la red, por ejemplo, con un equipo portátil o en caso de que se produzca un error del enrutador.

Si se utilizan carpetas redirigidas de cualquier tipo, es recomendable configurar Archivos sin conexión como se describe en la tabla siguiente.

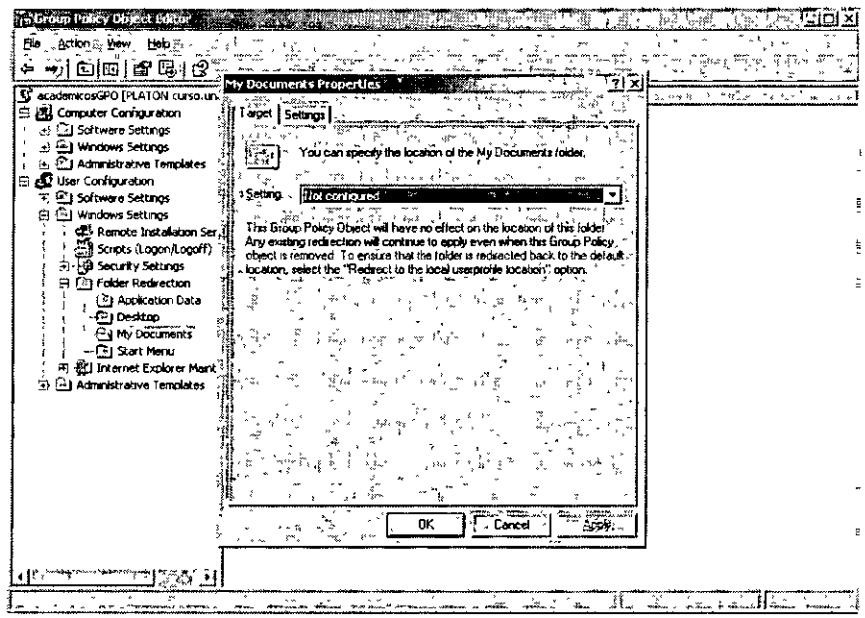
Carpeta especial	Configuración de Archivos sin conexión
Mis documentos	Caché automática para documentos (o caché manual para documentos si desea que los usuarios pongan disponibles manualmente los archivos y carpetas para su uso sin conexión)
Mis imágenes	Caché automática para documentos (o caché manual para documentos si desea que los usuarios pongan disponibles manualmente los archivos y carpetas para su uso sin conexión)
Datos de programa	Caché automática para programas

Carpeta especial	Configuración de Archivos sin conexión
Escritorio	Caché automática para programas si el escritorio es de Sólo lectura
Menú Inicio	Caché automática para programas

Redirigir Mis documentos al directorio principal

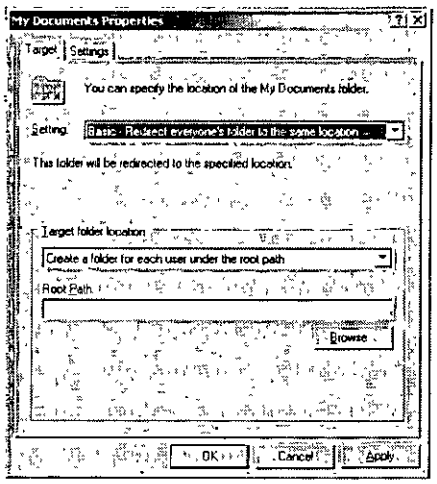
1. Abra un objeto de directiva de grupo vinculado al sitio, dominio o unidad organizativa que contiene los usuarios cuyas carpetas Mis documentos desea redirigir.

2. En el árbol de la consola, haga doble clic en **Fólder Redirection** para mostrar My Documents



3. Haga clic con el botón secundario del *mouse* (ratón) en **My documents** y, a continuación, haga clic en **Properties.**

4. En **Configuración**, en la ficha **Target**, haga clic en **Basic: redirect everyone´s fólder to the same location.**

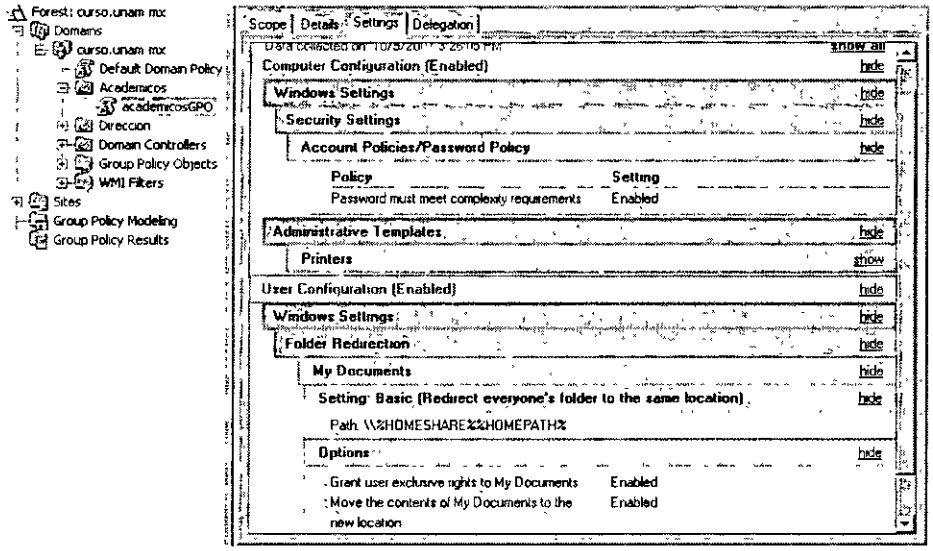


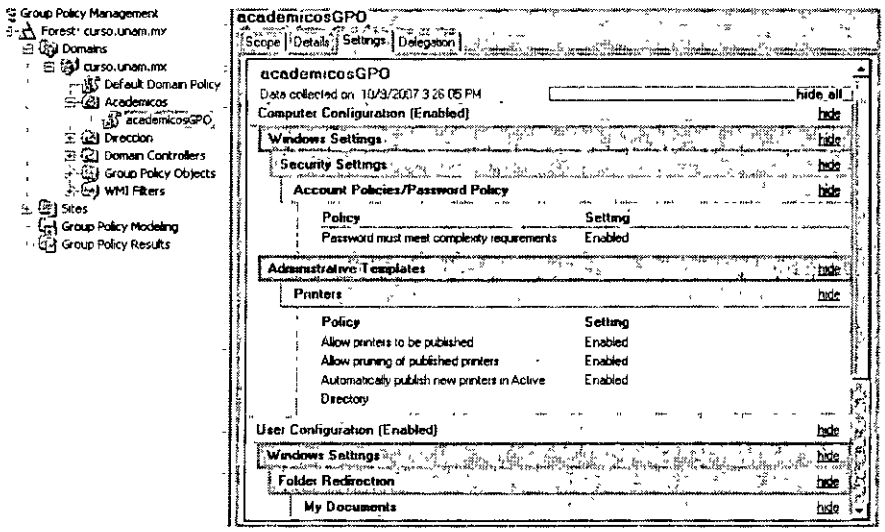
5. En **Target folder location**, haga click en **Redirect to the users home directory** y, a continuación, en **OK.**

Determinar los GPO (objetos de la directiva de grupo) aplicados

Para determinar las GPO´s aplicadas dentro de las directivas de grupo que están configuradas es mediante la herramienta de Consola de administración de Directivas de grupo (GPMC).

1. Seleccionar el objeto del cual se quiere ver que grupo de políticas se le están aplicando en Active Directory Users and Computer.
2. Clic derecho sobre el objeto para desplegar la venta de Properties, aquí seleccionar la pestaña de Group Policy. En esta ventana pulsar sobre open para abrir la GPMC.
3. En la consola seleccionar el grupo de políticas que se tienen asignadas.
4. En la parte de la derecha seleccionar la pestaña de Settings.
5. Aparecerán de manera resumida las políticas que se tienen habilitadas.





Consejos prácticos para administrar grupos de políticas

¿Cómo debo implementar las GPO's?

Se tiene que tener en cuenta principalmente la estructura presente y futura de la organización que se administra, la estructura administrativa del dominio y la forma deseada de procesamiento en sí de las directivas, para crear el modelo que mejor responda a nuestras necesidades e intereses. Como las herramientas para establecer las políticas en el dominio son las GPO's, que son conjuntos de una o más políticas, lo primero definiremos los tipos de GPO's según su diseño, para posteriormente estudiar las estrategias según diferentes conceptos.

¿Qué tipos de diseños tenemos de GPO's

Tenemos tres tipos de diseños de GPO's según las políticas que configuran:

1. ***GPO de directiva única***: cuando está orientada a un solo tipo de configuración (por ejemplo propiedades de Active Desktop). Es adecuado para organizaciones que delegan responsabilidades administrativas en muchos usuarios.

2. ***GPO de directiva múltiple***: cuando está orientada a varios tipos de configuración (por ejemplo, configuración de IE, de explorador de Windows, de instalación de software, etc.). Adecuado para organizaciones en las que la administración esté centralizada.

3. ***GPO de directiva dedicada***: cuando configura sólo políticas de equipo o de usuario. Aumenta el número de GPO's a ser procesadas en el inicio de sesión, alargando éste, pero es útil para aislar los problemas en la aplicación de una GPO.

¿Qué estrategias de aplicación de GPO's hay?

Hay dos estrategias de en función de cómo serán aplicadas las GPO's:

1. ***Por capas***: en esta estrategia se busca el que aparezca en el menor número posible de GPO's un tipo de configuración en concreto. De esta manera, se parte de una política común a todo el dominio aplicada a éste, en la cual no aparecen las configuraciones que son individuales para una OU .Pongamos que la configuración de escritorio es diferente en cada OU y la configuración de Proxy para el Internet Explorer es igual en todas las OU's; definiríamos a nivel de dominio la configuración de Proxy (ya sea con una GPO de directiva única o unida con otras directivas comunes a todas las OU's en una directiva múltiple) y crearíamos una GPO por OU con la configuración de escritorio propia de la OU en una directiva única:

a. **Ventaja**: La administración es más simple, al estar localizados perfectamente los puntos de aplicación de cada configuración y ser más fácil realizar cambios por tener que hacerlo en menos GPO's.

b. **Inconveniente**: El tiempo de inicio de sesión se alarga, al tener que procesarse múltiples GPO's.

c. **Adecuado...**: Para organizaciones cuya configuración de seguridad es común y con cambios frecuentes de directivas.

2. ***Monolítico***: Lo que se busca con este enfoque es que se apliquen el menor número posible de políticas; el ideal sería que se aplique tan sólo una. Para ello se configura una única GPO de directiva múltiple en cada OU y no se aplica GPO alguna en el dominio.

a. **Ventaja**: el inicio de sesión está optimizado para que sea lo más rápido posible.

b. **Desventaja**: la administración es más trabajosa; si necesitamos hacer un cambio de configuración común a todo el dominio, tendremos que retocar tantas GPO's como OU's tengamos.

c. **Adecuado...**: Para organizaciones en las cuales se pueden clasificar en muy pocos grupos la asignación de las directivas (digamos pocas OU's,) de forma que el aumento de las tareas administrativas orientadas a las directivas no sea preocupante.

¿Qué estrategias hay en función del trabajo?

En función de la forma de la organización de realizar su trabajo, hay dos estrategias:

1. ***Por roles***: Se utiliza una estructura de OU's que refleje los tipos de trabajo de la organización, como pueda ser comerciales, administrativos, marketing, etc. Aplicando el menor número posible de GPO's. Digamos que es un diseño por capas en el cual las GPO's de directiva única de las OU's son fusionadas en una única GPO de directiva múltiple por OU.

a. **Ventaja**: Los inicios de sesión son más rápidos que en una estrategia por capas.

b. **Desventaja**: La administración es algo más trabajosa que en una estrategia por capas.

c. **Adecuado...**: Para organizaciones en las cuales el trabajo está muy definido en función a roles.

2. ***Por equipos***: Se basa en vincular todas las GPO's al dominio en vez de a las OU's; el alcance de las GPO's se filtrará en base a grupos de seguridad. De esta forma se aplicarán una GPO a todos los usuarios pertenecientes a un grupo de seguridad determinado independientemente de la OU a la que pertenezcan.

a. **Ventajas**: Se minimizan las vinculaciones de GPO's a OU's y se centraliza la administración de las GPO's.

b. **Desventaja**: El inicio de sesión será más lento cuantos más equipos de trabajo existan.

c. **Adecuado...**: Para organizaciones en las que no corresponda el trabajo a realizar según roles, sino según tareas (por ejemplo, en un proyecto de desarrollo de software habrá desarrolladores, comerciales, administrativos, directivos, etc., que necesitarán determinadas configuraciones comunes a ellos, como la carpeta del proyecto.

Un comercial puede estar en más de un proyecto y necesitar acceso a las carpetas de los proyectos en los que está implicado). También es adecuado cuando se quiere que la administración de las políticas esté centralizada y sea muy flexible a las cambiantes necesidades de la organización.

¿Qué estrategias hay en función del tipo de control?

Cuando utilizamos la delegación del control de las GPO's tenemos dos estrategias para realizarlo, que se corresponden con los diseños:

1. ***Diseño de control centralizado***: En este diseño los administradores de OU tienen delegado el control de las GPO's, pero a su vez se conserva un control centralizado. Para hacerlo, las políticas a nivel de dominio llevarán activada la opción "No reemplazar". Es útil para organizaciones que quieren que los administradores de OU's tengan libertad de acción pero, a su vez, haya configuraciones comunes a todo el dominio que no puedan ser bloqueadas.

2. ***Diseño de control distribuido***: Cuando, además de tener control de su OU, un administrador de OU pueda bloquear las políticas del dominio. Es adecuado para organizaciones que quieren minimizar el número de dominios sin perder la autonomía de las OU's. A pesar de la capacidad de los administradores de OU de bloquear políticas, determinadas configuraciones, como por ejemplo de seguridad, siguen pudiendo estar centralizadas cuando se active en ellas la opción "No reemplazar".

¿Qué estrategia seguir?

Estas estrategias que hemos descrito, no son más que una categorización de estrategias según las necesidades y prestaciones deseadas. Cada organización es un caso totalmente distinto, y por ello, cada organización deberá llevar la estrategia que más le convenga. En algunos casos la estrategia deseable será alguna de las estrategias anteriores tal y como han sido descritas; en otras habrán de ser personalizadas y a veces habrán de mezclarse dos o más de ellas, e incluso estando retocadas las integrantes de la mezcla.

WINDOWS 2003 SERVER ®

Tema 11

Implementación de Plantillas Administrativas y una Directiva de Auditoria

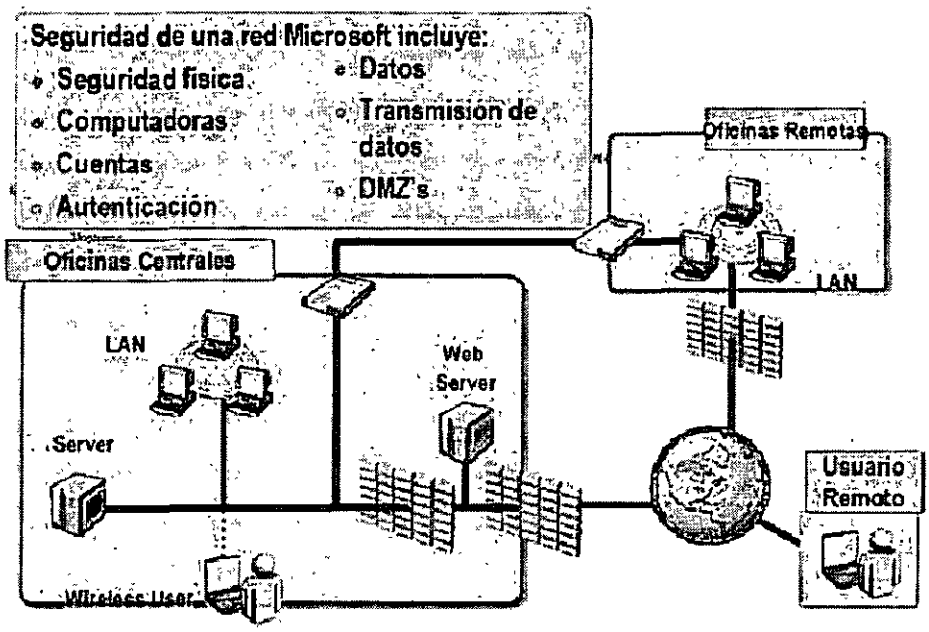
- Introducción a la seguridad en Windows Server 2003 ®
- Utilizar plantillas de seguridad para equipos de seguros
- Comprobar las directivas de seguridad de un ordenador
- Configurar la auditoria
- Administrar registros de seguridad

FLORES ALVARES LUIS ARMANDO
GUERRERO MARTINEZ EDSON ARMANDO

Introducción a la seguridad en Windows Server 2003 ®

Las empresas han ampliado sus redes tradicionales de área local (LAN) mediante la combinación de sitios de Internet, intranets y extranets. Como resultado, una mayor seguridad de los sistemas resulta ahora más importante que nunca.

Para proporcionar un entorno informático seguro, el sistema operativo Windows Server 2003 ® aporta muchas características nuevas e importantes de seguridad sobre aquellas incluidas originalmente en Windows 2000 Server ®.



Informática de confianza

Los virus existen y por ello que la seguridad del software es un reto constante. Para hacer frente a éstos, Microsoft ha convertido la informática de confianza en una iniciativa clave para todos sus productos. La informática de confianza es un marco para desarrollar dispositivos basados en equipos y software seguros y confiables, como los dispositivos y aparatos domésticos que utilizamos diariamente. Aunque en la actualidad no exista ninguna plataforma de informática de confianza, el nuevo diseño básico de Windows Server 2003 ® es un paso sólido hacia la conversión de este concepto en realidad.

Lenguaje común en tiempo de ejecución

El motor de software del lenguaje común en tiempo de ejecución es un elemento clave de Windows Server 2003 ® que mejora la confiabilidad y facilita un entorno informático

seguro. Asimismo reduce el número de errores y los agujeros de seguridad causados por errores comunes de programación, posibilitando que existan menos vulnerabilidades que los atacantes puedan explotar.

El lenguaje común en tiempo de ejecución verifica que las aplicaciones puedan realizarse sin errores, y a la vez comprueba los permisos de seguridad adecuados, asegurando que el código realice exclusivamente las operaciones correctas. Esto se lleva a cabo comprobando aspectos como los siguientes: la ubicación desde la cual se ha descargado o instalado el código, si el código tiene una firma digital de un desarrollador de confianza, y si el código ha sido alterado desde su firma digital.

Windows Server 2003 ® proporciona muchas características nuevas y mejoradas que se combinan para crear una plataforma más segura para llevar a cabo actividades empresariales.

Característica	Descripción
Servidor de seguridad de conexión a Internet	Windows Server 2003 ® proporciona seguridad de Internet mediante el uso de un servidor de seguridad basado en software, llamado Servidor de seguridad de conexión a Internet (ICF). El ICF proporciona protección a los equipos conectados directamente a Internet o a los equipos ubicados detrás de un equipo host de conexión compartida a Internet (ICS) y que ejecute un ICF.
Servidor de seguridad de conexión a Internet	Windows Server 2003 ® proporciona seguridad de Internet mediante el uso de un servidor de seguridad basado en software, llamado Servidor de seguridad de conexión a Internet (ICF). El ICF proporciona protección a los equipos conectados directamente a Internet o a los equipos ubicados detrás de un equipo host de conexión compartida a Internet (ICS) y que ejecute un ICF.
Servidor IAS/RADIUS seguro	El Servidor de autenticación de Internet (IAS) es un Servidor de usuario de acceso telefónico de autenticación remota (RADIUS) que administra la autorización y la autenticación del usuario. También administra conexiones con la red mediante el uso de diversas tecnologías de conectividad, como el acceso telefónico, las redes privadas virtuales (VPN) y los servidores de seguridad.
Redes LAN Ethernet e inalámbricas seguras	Windows Server 2003 ® permite la autenticación y la autorización de usuarios y equipos que se conectan a redes LAN Ethernet e inalámbricas. Esto es posible por la compatibilidad de Windows Server 2003 ® con los protocolos IEEE 802.1X. (Los estándares IEEE 802 definen métodos para obtener acceso a redes LAN y controlarlas.)
Directivas de restricción de software	Windows Server 2003 ® permitirá que un administrador de sistemas utilice la exigencia de directivas o ejecución para prevenir que se lleven a cabo en un equipo programas ejecutables. Por ejemplo, aplicaciones específicas de ámbito corporativo pueden ver su ejecución restringida a menos que se ejecuten desde un directorio específico. Las directivas de restricción de software también pueden configurarse para prevenir la ejecución de código mal intencionado o infectado por virus.
Directivas de restricción de software	Windows Server 2003 ® permitirá que un administrador de sistemas utilice la exigencia de directivas o ejecución para prevenir que se lleven a cabo en un equipo programas ejecutables. Por ejemplo, aplicaciones específicas de ámbito corporativo pueden ver su ejecución restringida a menos que se ejecuten desde un directorio específico. Las directivas de restricción de software también pueden configurarse para prevenir la ejecución de código mal intencionado o infectado por virus.
Mejoras de la seguridad para servidores en redes LAN Ethernet e inalámbricas	Windows Server 2003 ® proporciona seguridad para redes LAN Ethernet e inalámbricas basadas en las especificaciones IEEE 802.11 y que sean compatibles con certificados públicos implementados mediante la

	inscripción automática o las tarjetas inteligentes. Estas mejoras en la seguridad permiten el control de la obtención de acceso a redes Ethernet en lugares públicos, como centros comerciales o aeropuertos. La autenticación de equipos también se admite en un entorno operativo de protocolo de autenticación extensible (EAP).
Seguridad aumentada para servidores Web	La seguridad de la información es un problema de vital importancia para las organizaciones de todo el mundo. Para aumentar la seguridad de los servidores Web, los Servicios de Internet Information Server 6.0 (IIS 6.0) se configuran para obtener la máxima seguridad. Su instalación predeterminada es el estado "bloqueado". Las características de seguridad avanzada de IIS 6.0 incluyen: servicios criptográficos que se pueden seleccionar, autenticación de síntesis avanzada y control configurable de la obtención de acceso a los procesos. Estas son sólo algunas de las tantas características de seguridad que le permitirán realizar negocios de forma segura en la Web.

Módulo criptográfico	Procesamiento de Información (FIPS). Entre estos algoritmos cabe incluir: SHA-1, DES, 3DES y un generador de número aleatorio aprobado. El módulo criptográfico, compatible con FIPS de modo de núcleo, permite que las organizaciones gubernamentales implementen Seguridad de Protocolo Internet (IPSec) compatible con FIPS 140-1. Para ello deberán utilizar: Servidor y cliente de VPN L2TP (Protocolo de túnel de capa 2)/IPSec. Túneles L2TP/IPSec para conexiones VPN entre puertas de enlace. Túneles IPSec para conexiones VPN entre puertas de enlace. Tráfico de red de extremo a extremo, cifrado mediante IPSec, entre cliente y servidor, y de servidor a servidor.
Nuevo paquete de seguridad de síntesis	El nuevo paquete de seguridad de síntesis es compatible con el protocolo de autenticación de síntesis, junto con RFC 2617 y RFC 2222. Estos protocolos son compatibles con Microsoft Internet Information Server (IIS) y el servicio Active Directory. Mejoras en la seguridad de los sistemas Se han realizado importantes mejoras para garantizar una seguridad general de los sistemas, incluyendo: Mejoras del rendimiento en un 35 por ciento, al utilizar la capa de sockets segura (SSL). IIS no se instala de forma predeterminada. Para implementar IIS, primero debe instalarse mediante la opción Agregar o quitar programas del Panel de control. Capacidad de comprobación del búfer de Microsoft Visual Studio®. (Los piratas informáticos utilizan habitualmente las saturaciones del búfer para explotar un sistema.)
Credenciales	El administrador de credenciales de Windows Server 2003 ® proporcionará un almacén seguro para las credenciales del usuario, incluyendo contraseñas y certificados X.509. Estas credenciales proporcionan una experiencia sólida de inicios de sesión únicos para los usuarios, incluidos los usuarios móviles. Una API de Win32® se encuentra disponible para permitir que las aplicaciones basadas en cliente o en servidor obtengan credenciales del usuario.
Mejoras en la autenticación de clientes SSL	En Windows Server 2003 ®, la caché de sesión SSL puede compartirse mediante múltiples procesos. Esto reduce el número de veces que un usuario tiene que volver a autenticarse en las aplicaciones, y asimismo reduce los ciclos de CPU en el servidor de aplicaciones.

La mejor plataforma para la infraestructura de claves públicas

Característica	Descripción
Renovación automática e inscripción automática de certificados	Estas nuevas características importantes reducen de forma drástica la cantidad de recursos necesarios para administrar certificados X.509. Windows Server 2003 ® posibilita la inscripción e implementación automática de certificados para los usuarios. Asimismo cuando el certificado caduque, podrá renovarse en forma automática. La renovación automática e inscripción automática de certificados facilita la implementación más rápida de tarjetas inteligentes y mejora la seguridad de las conexiones inalámbricas (IEEE 802.1X) mediante la caducidad y renovación automática de certificados.
Compatibilidad de Windows Installer con la firma digital	La compatibilidad con la firma digital permite que los paquetes y contenedores externos de Windows Installer se firmen digitalmente. Esto proporciona a los administradores de tecnologías de la información, unos paquetes de Windows Installer más seguros, resultando de suma importancia si el paquete se envía a través de Internet.
Mejoras en las listas de revocación de certificados (CRL)	El servidor de certificados incluido en Windows Server 2003 ® ahora es compatible con las CRL delta. Una CRL hace que la publicación de certificados X.509 revocados sea más eficaz, y facilita que un usuario pueda recuperar un certificado nuevo. Y como ahora se puede especificar la ubicación en la cual se encuentra almacenada la CRL, resulta más fácil moverla para albergar las necesidades de seguridad y empresariales específicas.

Extensión segura de las actividades empresariales en Internet

Característica	Descripción
Integración con 'Passport'	Puede asignarse una identidad de Passport a una identidad de Active Directory en Windows Server 2003 ®. Por ejemplo, la asociación de una identidad de Passport con una identidad de Active Directory permite que una empresa asociada pueda ser autorizada para obtener acceso a los recursos a través de IIS, en lugar de tener que iniciar sesión directamente en una red de Windows. La integración con Passport proporcionará una experiencia de inicio de sesión única, mediante el uso de IIS.
Relaciones de confianza entre bosques	Si trabaja con un asociado o una empresa que ha implementado un bosque de Active Directory, puede utilizar Windows Server 2003 ® para configurar una relación de confianza entre los bosques del asociado o la empresa y sus propios bosques. Esto le permite confiar de forma explícita en algunos usuarios, en grupos o en todos, los que pertenezcan a otro bosque. También tiene la capacidad de establecer permisos en base a los usuarios o grupos que residen en el otro bosque. Las relaciones de confianza entre bosques facilitan la dirección de negocios con otras empresas mediante Active Directory.

Autenticación ante un equipo remoto

Autenticación en Windows 2000/2003 ®

Existen dos protocolos para la autenticación de red dentro de dominios de Windows 2000 ®.

Kerberos Version 5. Protocolo predeterminado para la autenticación de red en sistemas W2K.

Windows NT LAN Manager (NTLM). Protocolo predeterminado para la autenticación de red en NT 4.0. Es mantenido en 2000 y 2003 para compatibilidad con clientes y servidores de mas bajo nivel.

LM. Protocolo de autenticación desarrollado por Microsoft e IBM, su debilidad recae en lo siguiente:

- LM no distingue entre mayúsculas y minúsculas. Todas las letras son convertidas a mayúsculas ante de que el hash sea obtenido.
- LM divide la contraseña en dos cadenas de 7 caracteres y de cada uno se se obtiene un hash, por lo que los hash no tiene mas de 7 caracteres.
- Las contraseñas por lo tanto no pueden ser mayores de 14 caracteres.
- El protocolo LM utiliza DES y una cadena conocida para realizar el cifrado.

Beneficios

Mejores Prácticas - Autenticación ante un equipo remoto

- Implemente contraseñas complejas
- Bloqueo de Cuentas
- Habilite la auditoria de sucesos de inicio de sesión de cuenta
- Bloquee la cuenta autentica de Administrador y cree un señuelo
- Deshabilite las cuentas inactivas
- Deshabilitar el almacenar el hash LM en la sam mediante políticas
- La implementación de estas políticas se vera posteriormente

Utilizar plantillas de seguridad para equipos de seguros

Las plantillas de seguridad predefinidas se proporcionan como punto de partida para crear directivas de seguridad que se personalizan para cumplir los diferentes requisitos organizativos. Puede personalizar las plantillas con el complemento Plantillas de seguridad. Una vez personalizadas las plantillas de seguridad predefinidas, puede utilizarlas para configurar un equipo o muchos.

Puede configurar equipos individuales con el complemento Configuración y análisis de seguridad, la herramienta de línea de comandos Secedit o mediante la importación de la plantilla en Directiva de seguridad local. Puede configurar varios equipos si importa una plantilla en Extensión Configuración de seguridad para Directiva de grupo, que es una extensión de Directiva de grupo. También puede usar una plantilla de seguridad como referencia para analizar un sistema en busca de posibles brechas en la seguridad o infracciones de directivas, mediante el complemento Configuración y análisis de seguridad. De forma predeterminada, las plantillas de seguridad predefinidas están almacenadas en:

raízDelSistema\Security\Templates

Seguridad predeterminada (Setup security.inf)

La plantilla Setup security.inf se crea durante la instalación en cada equipo. Puede variar de un equipo a otro, en función de si la instalación fue limpia o una actualización. Setup security.inf representa la configuración de seguridad predeterminada que se aplicó durante la instalación del sistema operativo, incluyendo los permisos de archivo para la raíz de la unidad del sistema. Se puede usar en servidores y equipos cliente; no se puede aplicar a controladores de dominio. Puede aplicar partes de esta plantilla para la recuperación de desastres.

Setup security.inf nunca se debería aplicar a través de Directiva de grupo. Contiene una gran cantidad de datos y puede afectar seriamente al rendimiento si se aplica a través de Directiva de grupo, ya que la directiva se actualiza periódicamente y se movería una gran cantidad de datos por el dominio.

Es aconsejable aplicar la plantilla Setup security.inf por partes. Dado que la herramienta de línea de comandos Secedit le proporciona esta opción, se recomienda utilizarla.

Seguridad predeterminada del controlador de dominio (DC security.inf)

Esta plantilla se crea cuando un servidor se promueve a controlador de dominio. Refleja la configuración de seguridad predeterminada de loa archivos, el Registro y los servicios del sistema. Cuando se vuelve a aplicar, se restablecen los valores predeterminados estas áreas, pero puede reemplazar los permisos para nuevos archivos, claves del Registro y servicios del sistema que otras aplicaciones hayan creado. Se puede aplicar mediante el complemento Configuración y análisis de seguridad o con la herramienta de línea de comandos Secedit.

Compatible (Compatws.inf)

Los permisos predeterminados para estaciones de trabajo y servidores se conceden principalmente a tres grupos locales: Administradores, Usuarios avanzados y Usuarios.

Los administradores tienen la mayor parte de los privilegios mientras que los usuarios son los que tienen menos. Por ello, puede mejorar notablemente la seguridad, confiabilidad y el costo total de la propiedad si:

- Se asegura de que los usuarios finales sólo son miembros del grupo Usuarios.
- Implementa aplicaciones que los miembros del grupo Usuarios pueden ejecutar correctamente.

Quienes disponen de privilegios de usuario pueden ejecutar correctamente las aplicaciones que formen parte del programa del logotipo de Windows para software. Sin embargo, es posible que el grupo Usuarios no pueda ejecutar las aplicaciones que no cumplan los requisitos del programa. Si tiene que usar otras aplicaciones, dispone de dos opciones:

- Permitir que los miembros del grupo Usuarios lo sean también del grupo Usuarios avanzados.
- Aumentar los permisos predeterminados que concede al grupo Usuarios.

Como el grupo Usuarios avanzados tiene capacidades inherentes, como crear usuarios, grupos, impresoras y recursos compartidos, algunos administradores preferirían aumentar los permisos predeterminados de dicho grupo antes que permitir que los usuarios finales sean miembros del mismo. Esto es precisamente lo que hace la plantilla compatible. Cambia los permisos predeterminados de archivos y del Registro que se conceden al grupo Usuarios de forma que sean coherentes con los requisitos de la mayor parte de las aplicaciones que no pertenecen al programa del logotipo de Windows para software. Además, puesto que se supone que el administrador que aplica la plantilla compatible no desea que los usuarios finales sean Usuarios avanzados, la plantilla compatible quita todos los miembros del grupo Usuarios avanzados.

La plantilla compatible no debería aplicarse a controladores de dominio. Por ejemplo, no la importe en la directiva Dominio predeterminado o la directiva Controlador de dominio predeterminado de Directiva de grupo.

Segura (Secure*.inf)

La plantilla segura define una configuración de seguridad mejorada que afecta menos a la compatibilidad de las aplicaciones. Por ejemplo, la plantilla segura define configuraciones de contraseña, bloqueo y auditoría más rigurosas.

Además, las plantillas Segura limitan el uso de los protocolos de autenticación LAN Manager y NTLM, al configurar los clientes para que sólo envíen respuestas NTLMv2 y configurar los servidores para que rechacen las respuestas de LAN Manager.

- Para aplicar Securews.inf a un equipo miembro, todos los controladores de dominio que contienen las cuentas de todos los usuarios que inician una sesión en el cliente deben ejecutar Windows NT 4.0 ® Service Pack 4 o posterior.

- Para aplicar Securews.inf a un equipo miembro que se ha unido a un dominio que contiene controladores de dominio que ejecutan Windows NT 4.0 ®, los relojes de los controladores de dominio que ejecutan Windows NT 4.0 ® y los equipos miembro deben estar desincronizados 30 minutos.

- Si un cliente se configura con Securews.inf, no podrá conectar con servidores que sólo utilizan el protocolo de autenticación de LAN Manager o que ejecutan Windows NT 4.0 ® anterior a Service Pack 4 con una cuenta local definida en el servidor de destino.

- Si un cliente se configura con Securews.inf, no podrá conectar con servidores que ejecuten Windows 2000 ® o Windows NT 4.0 ® mediante una cuenta local definida en el servidor de destino a menos que el reloj de dicho servidor esté desincronizado 30 minutos con respecto al reloj del cliente.

- Si un cliente está configurado con Securews.inf, no podrá conectar con un equipo en el que se utilice Windows XP ® o posterior mediante una cuenta local definida en el servidor de destino a menos que el reloj de dicho servidor esté desincronizado 20 horas con respecto al reloj del cliente.

- Si un cliente se configura con Securews.inf, no podrá conectar con servidores que usen LAN Manager y se estén ejecutando en modo de seguridad en el nivel de recursos.

- Si un servidor se configura con Securews.inf, entonces un usuario con una cuenta local en ese servidor no podrá conectarse a él desde un equipo cliente que sólo ejecute LAN Manager y esté utilizando esa cuenta local.

- Si un servidor en el que se ejecuta Windows 2000 ® se configura con securews.inf, un cliente con una cuenta local en ese servidor que esté también configurado para utilizar autenticación NTLMv2 no podrá conectarse a menos que los relojes de los dos equipos estén desincronizados 30 minutos.

- Si un servidor en el que se ejecuta Windows XP ® se configura con securews.inf, un cliente con una cuenta local en ese servidor que esté también configurado para utilizar autenticación NTLMv2 no podrá conectarse a menos que los relojes de los dos equipos estén desincronizados 20 horas.
- Si un controlador de dominio se configura con Securedc.inf, un usuario con una cuenta en ese dominio no podrá conectar con ningún servidor miembro desde un equipo cliente que sólo ejecute LAN Manager con esa cuenta de dominio.

- Los equipos que ejecutan LAN Manager incluyen Windows para Trabajo en Grupo, así como las plataformas Windows 95 ® y Windows 98 ® que no disponen del Paquete de extensiones de cliente de Active Directory instalado. Si el Paquete de extensiones de cliente de Active Directory está instalado en Windows 95 ® o Windows 98 ®, estos clientes podrán utilizar NTLMv2. Windows Millennium Edition ® es compatible con NTLMv2 sin ninguna modificación adicional necesaria.

- Los equipos en los que se ejecuta Windows NT Service Pack 4 o posterior se pueden configurar para enviar sólo respuestas NTLMv2; para ello, defina **HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel** con un valor de 3 o superior.

- Los equipos en los que se ejecuta Windows NT Service Pack 4 o posterior se pueden configurar para enviar sólo respuestas NTLMv2; para ello, especifique esta preferencia en la opción de seguridad Seguridad de red: nivel de autenticación de LAN Manager.

Las plantillas seguras también restringen más a los usuarios anónimos al impedir que éstos (por ejemplo, los usuarios de un dominio que no es de confianza):

- Enumeren nombres de cuentas y de recursos compartidos.
- Realicen traducciones de SID a nombre o de nombre a SID.

Finalmente, las plantillas seguras (Secure) permiten firmar paquetes de Bloque de mensajes de servidor (SMB) en el servidor, lo que está deshabilitado de forma predeterminada en los servidores. Como el firmado de paquetes SMB en el cliente está habilitado de forma predeterminada, la firma de paquetes SMB siempre se negocia cuando las estaciones de trabajo y los servidores operan en el nivel Seguro.

De alta seguridad (hisec*.inf)

Las plantillas de alta seguridad son superconjuntos de plantillas seguras que imponen mayores restricciones en los niveles de cifrado y firmado que se requieren para la autenticación y para los datos que fluyen en canales protegidos y entre clientes y servidores SMB. Por ejemplo, mientras que las plantillas seguras hacen que los servidores rechacen las respuestas de LAN Manager, las plantillas de alta seguridad provocan que los servidores rechacen las respuestas de LAN Manager y de NTLM. Aunque la plantilla segura permite la firma de paquetes SMB en el servidor, la plantilla de alta seguridad la requiere. Además, las plantillas de alta seguridad requieren un cifrado y firma seguros en los datos del canal protegido que constituye las relaciones de confianza de dominio a miembro y de dominio a dominio. Por lo tanto, para aplicar hisecws.inf a un equipo miembro:

- Todos los controladores de dominio que contengan las cuentas de todos los usuarios que iniciarán sesión en el cliente tienen que ejecutar Windows NT 4.0 ® Service Pack 4 o posterior.
- Todos los controladores de dominio del dominio al que está unido el cliente deben ejecutar Windows 2000 ® o posterior.
- Los clientes que se configuran con Hisecws.inf no pueden conectar con equipos que sólo ejecuten LAN Manager o con equipos que ejecuten Windows NT ® 4.0, Service Pack 3 o anterior mediante una cuenta local definida en el servidor de destino.
- Los clientes que se configuran con Hisecws.inf no pueden conectar con servidores que ejecuten Windows 2000 ® o Windows NT 4.0 ® Service Pack 4 mediante una cuenta local definida en el servidor de destino a menos que el reloj de dicho servidor esté desincronizado 30 minutos con respecto al del cliente.
- Los clientes que se configuran con Hisecws.inf no pueden conectar con equipos en los que se use Windows XP ® o posterior mediante una cuenta local definida en el equipo de destino a menos que el reloj de dicho servidor esté desincronizado 20 horas con respecto al del cliente.
- Los clientes que se configuran con Hisecws.inf no pueden conectar con servidores LAN Manager que funcionen en modo de seguridad de nivel de recursos.
- Para aplicar Hisecdc.inf a un controlador de dominio, todos los controladores de dominio de todos los dominios de confianza o que confían deben ejecutar Windows 2000 ® o sistemas operativos de la familia de Windows Server 2003 ®.
- Si un servidor se configura con Hisecws.inf, un usuario con una cuenta local en dicho servidor no podrá conectar con él desde un cliente que no sea compatible con NTLMv2.
- Si un servidor se configura con Hisecws.inf, un cliente con una cuenta local en dicho servidor no podrá conectar con él a menos que el equipo del cliente se configure para enviar respuestas NTLMv2.
- Si un servidor se configura con Hisecws.inf, todos los clientes que vayan a utilizar SMB para conectar con él tienen que habilitar la firma de paquetes SMB en el cliente. Todos los equipos con los sistemas operativos Windows 2000 ® y Windows XP ® habilitan la firma de paquetes SMB en el cliente de forma predeterminada.
- Si un controlador de dominio se configura con Hisecdc.inf, un usuario con una cuenta en ese dominio no puede conectar con servidores miembros con esa cuenta de usuario de dominio si se está intentando establecer la conexión desde un cliente que sólo utiliza el protocolo de autenticación de LAN Manager
- Si un controlador de dominio se configura con Hisecdc.inf, un usuario con una cuenta en dicho dominio no podrá conectar con servidores miembros con esa cuenta de dominio a menos que:

El cliente y el servidor de destino estén ejecutando Windows 2000 ® o posterior, y puedan utilizar la autenticación Kerberos en lugar de la autenticación basada en LAN Manager.

El cliente esté configurado para enviar respuestas NTLMv2.

Precaución

Estas plantillas de seguridad están construidas con la suposición de que se van a aplicar en equipos que utilizan la configuración de seguridad predeterminada. En otras palabras, modifican gradualmente la configuración de seguridad predeterminada, si el equipo la tiene. *No* instalan la configuración de seguridad predeterminada antes de hacer las modificaciones.

Las plantillas de seguridad predefinidas no deben aplicarse a los sistemas de producción sin haberlas probado para garantizar que mantienen la funcionalidad correcta para la arquitectura del sistema y la red.

La configuración de la plantilla de seguridad se puede ver en Plantillas de seguridad. Los archivos *.inf también se pueden ver como archivos de texto. Dichos archivos se encuentran en:

%windir%\Security\Templates

Plantillas de seguridad

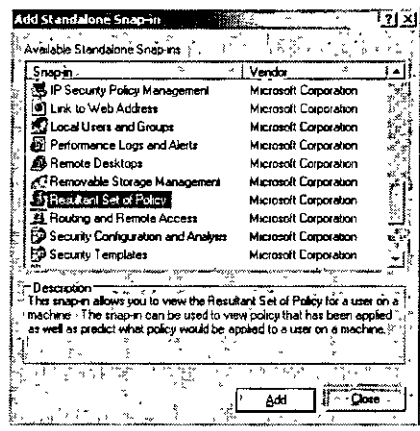
1. Para crear una nueva consola, vaya a **Start** luego **run** y escriba **mmc** y **OK**. Entonces se abrirá una consola para utilizar las plantillas.
2. En el menú de **File** seleccione la opción de **Add/Remove Snap-in**. Luego pulse en **Add** para añadir una plantilla.
3. Aparecerá un cuadro de selección, aquí debemos seleccionar la opción de **Security Templates** y de clic en **Add**.
4. Luego cierre con **Close**. Y **Ok** después.
5. Seleccione del menú de la consola de **File,** la opción de **Save** y póngale nombre a la consola que se esta creando y guarde.
6. De doble clic sobre la opción de **Security Templates** en la consola y expanda la carpeta que se encuentra en el menú.
7. Aparecerá la lista de las opciones de las plantillas de seguridad que trae por default Windows 2003 Server ®.
8. Seleccione alguna y con clic derecho pulse en **open.**
9. Aparecerán las políticas de seguridad que trae la plantilla.
10. Estado aquí podemos habilitar o deshabilitar las opciones que necesitemos y utilizar las que más se adecuen a nuestras necesidades.
11. Después de haber cambiado algunos valores podemos guardar esta plantilla para su posterior uso.
12. Seleccionamos la plantilla que acabamos de modificar y con clic derecho sobre ella aparecerá el menú contextual en donde seleccionamos **Save as** para ponerle nombre y poder utilizarla.

Comprobar las directivas de seguridad de una computadora

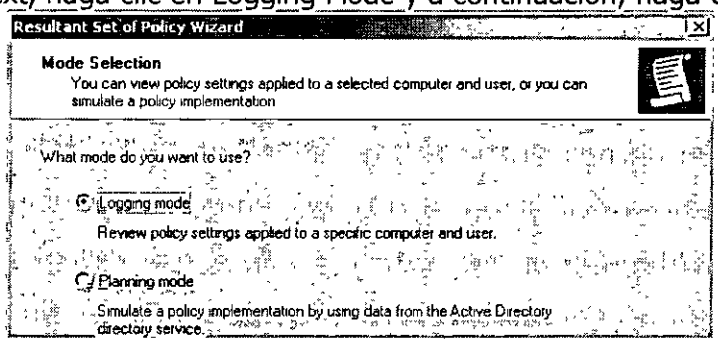
Para comprobar las directivas de seguridad que una computadora tiene habilitadas dentro del Active Directory utilizaR la utilidad Conjunto resultante de directivas (rsop.msc), puede recopilar sólo información de directiva del equipo necesarias:

1. Haga clic en Start, haga clic en run, escriba mmc en el cuadro y a continuación, haga clic en OK.
2. Haga clic en File, haga clic en Add/Remove Snapin y a continuación, haga clic en Add en el cuadro de diálogo Add or Remove Snapin.

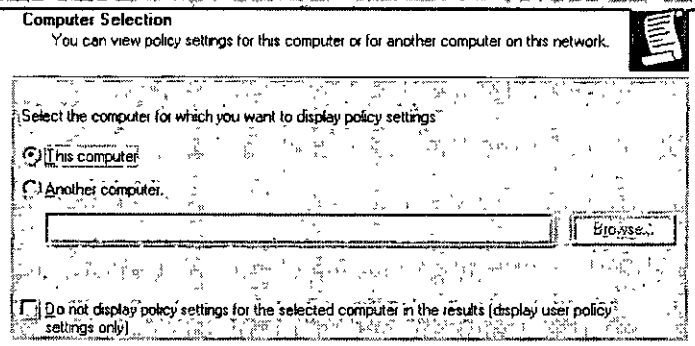
3. Haga clic en Resultant Set of Policy, haga clic en Add y a continuación, haga clic en Close en el cuadro de diálogo Add/Remove Standalone Snapin



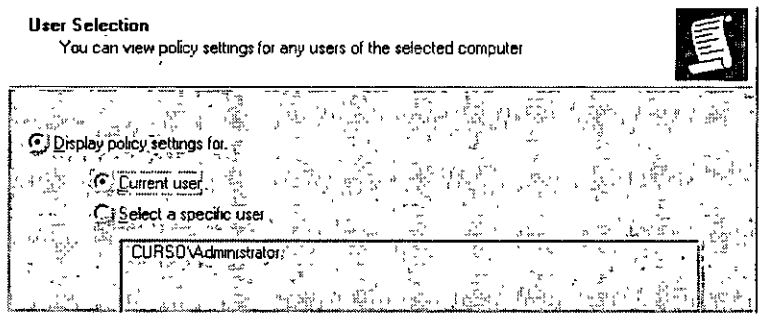
4. Haga clic en OK en los cuadros de diálogo Add or Remove Snapin. El complemento Conjunto resultante de directivas aparece en el MMC.
5. Haga clic en Generate RSOP data en el menú Action.
6. Haga clic en Next, haga clic en Logging Mode y a continuación, haga clic en Next.



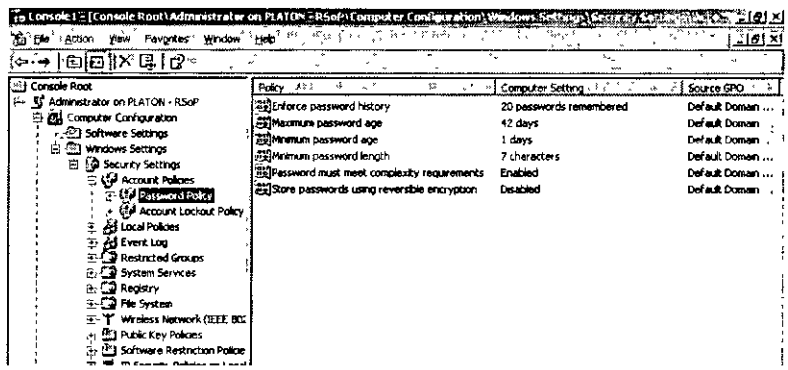
7. Haga clic en This Computer u otro equipo y a continuación, escriba el nombre de equipo.



8. Haga clic en Select a specific user y a continuación, haga clic en el espacio vacío que hay debajo de los usuarios incluidos en la lista. Esto tiene el mismo efecto para hacer clic en Do not display user policy settings in the results.



9. Haga clic en Next y, a continuación, en Next. Observe que las configuraciones sólo específicas del equipo aparecen.



Configurar la auditoria

¿Qué es la auditoria?

Proceso de guardar las actividades (llamadas eventos) de usuarios y del sistema operativo de un sistema de computo. Es necesario analizar estas actividades para evaluar todas las medidas de seguridad. Se debe de implementar la auditoria y monitorear los

eventos del sistema para detectar intentos de intuición que pueden comprometer los datos del sistema. Cuando ocurre un evento de auditoria, Windows escribe un registro del evento en el registro de la seguridad.

Cual es el objetivo de la auditoria

Establecer un seguimiento de auditoria es un aspecto importante en la seguridad. Controlar la creación o la modificación de objetos permite hacer un seguimiento de los problemas de seguridad potenciales, ayuda a asegurar la responsabilidad del usuario y proporciona pruebas en caso de una infracción de seguridad.

- Registrar el éxito o falla de los eventos
- Minimizar el riesgo de uso no autorizado de los recursos
- Mantener un registro de la actividad de los usuarios y de las cuentas administrativas

¿Qué pasa si no se audita?

Como parte de una estrategia de seguridad se debe de determinar el nivel de auditoria apropiado para el ambiente de cómputo. Si no se halla la Auditoria en un sistema de cómputo, un Administrador no puede ser capaz de tener control de las actividades que se realicen, es incapaz de detectar los problemas de seguridad y seria capaz de obtener información en el caso de que el sistema sea comprometido.

- No se tiene control de las actividades realizadas en el sistema.
- Los problemas de seguridad pueden ser difíciles de identificar.
- El sistema puede permanecer vulnerable a ataques.

Si se audita en exceso ¿Qué pasa?

Cuando se decide habilitar la auditoria, se deberá tener en cuenta que cuanto más alto sea el nivel (cuando se auditen mas eventos), mas sucesos se generaran y mas difícil resultara detectar secesos críticos.

Si se lleva a cabo una auditoria exhaustiva, se recomienda considerar el uso de herramientas adicionales, como Microsoft Operations Manager, para ayudarle a filtrar los sucesos de mayor importancia.

- Degradación en el desempeño del sistema
- Se puede ocultar eventos críticos
- La auditoria no es efectiva

Políticas de Auditoria

Se debe de establecer una política de auditoria adecuada, ya que si se audita demasiados tipos de eventos, se puede crear una sobrecarga en el sistema, afectando de esta forma el desempeño del mismo. Se recomienda que se auditen solo aquellos eventos que proporcionan información que es útil para controlar la seguridad.

- Determinar las computadoras en las que se configurara la auditoria
- Determinar los eventos a auditar
  - Accesos a archivos y carpetas
  - Conexión y desconexión de usuarios
  - Apagado y reinicio del servidor
- Cambios a cuentas de usuarios y grupos
- Determinar si se audita el éxito o fallo de eventos, o ambos.

Antes de habilitar la auditoria, debe establecerse los tipos de eventos que se van a auditar, la frecuencia en que se revisaran las bitácoras del sistema, así como establecer el personal encargado de recolectar y analizar el registro de seguridad en los sistemas.
Solo al personal confiable debe dársele el derecho de acceder al registro de seguridad, debido a que contiene información crítica para la organización.

- Determinar si es necesario registrar las tendencias del uso del sistema
- Revisar los registros de seguridad frecuentemente
- Minimizar el riesgo de uso no autorizado de los recursos
- Mantener un registro de la actividad de los usurarios y de las cuentas administrativas

Registros de auditoria

El subsistema de auditoria de Windows tiene seis registros. Existen tres registros que están presentes de forma predeterminada en todos los sistemas de Windows Aplicación, Sistema y Seguridad. Los otros tres, Servicio de Directorio, Replicación de Archivos y Servidor DNS están presentes solo si se han instalado los servicios apropiados.

Aplicación. Guarda los eventos producidos por las aplicaciones o programas.

Sistema. Contiene eventos producidos por el propio sistema y sus componentes.

Seguridad. Contiene información concerniente a los eventos del sistema, incluyendo información relativa a la monitorización de la actividad de los usuarios y procesos, igual que mensajes relativos a los servicios de seguridad.

Servicio de Directorio. Contiene información relativa al los servicios de directorio

Replicación de Archivos. Guarda los eventos relativos a la replicación de archivos.

Servidor DNS. Contiene información relativa al servicio DNS (Domain Name Server)

Se puede establecer independientemente la configuración de cada registro en términos de su tamaño máximo y lo que podría ocurrir cuando alcance este tamaño. Solamente en el caso del Registro de Seguridad se puede controlar lo que se guardara.

Categorías del registro de Auditoria

Independientemente del registro que visualice, el sistema de auditoria sitúa cada evento en una de cinco categorías:

Error. Indica eventos significativos, como perdida de funcionalidad o datos

Warning. Indica un evento que no es significativo, pero puede causar problemas en el futuro.

Information. Indica una operación realizada con éxito (servicio de una aplicación o dispositivo)

Success Audit. Indica un evento ocurrido ante un intento de éxito de auditoria.

Failure Audit. Indica un evento ocurrido cuando se ha producido un fallo de auditoria.

Directivas de auditoria

Audit account logon event. Registra los eventos de inicio y cierre de sesión de usuario en otras computadoras en los que la computadora local fue utilizada para autenticar la cuenta.

Audit account managenment. Rastrea los cambios hechos la base de datos de Security Account (cuando una cuenta es creada, cambiada o eliminada).

Audit directory service access. Audita los accesos de usuario a los objetos de Active Directory que tienen SACL´s (System Access Control List) definidas. Esta opción es similar a Audit Object Access excepto que solo aplica a objetos de Active Directory y no a objetos de archivo y Registry. Debido a que esta opción solo aplica a Active Directory, no tiene significado en estaciones de trabajo y servidores miembro.

Audit logon events. Registra los usuarios que han iniciado o cerrado sesión, o que han realizado una conexión de red. También registra el tipo de inicio de sesión requerido (interactivo, red o servicio). Esta opción se diferencia de Audit account logon events en que esta se registra donde ocurrió el inicio de sesión y no el lugar donde reside la cuenta.

Audit object access. Registra los intentos de acceso a objetos (directorios, archivos e impresoras). La auditoria de objetos individuales no es automática y debe ser habilitada en las propiedades del objeto.

Audit policy change. Registra en las actividades de seguridad, como lo son la asignación de privilegios o cambios en la directiva de la auditoria.

Audit privilege use. Registra los intentos de uso de privilegios. Los privilegios indican los derechos asignados a grupo Administrators o a otros usuarios poderosos. Rastrea todos lo derechos de usuario excepto: Bypass Traverse Checking, Debug Programs, Create a token Objet, Replace Process Level Token, Generate Security Audits, Back up Files and Directories, y Restore Files and Directories.

Audit process tracking. Registra información detallada de eventos como la activación de programas, salida de algún proceso, etc.

Para configurar una política de auditoria siga los siguientes pasos.

1. Selecciones del menú **Start, Programs, Admnistrative tools, Acitve Directory Users and Computers** y abra la consola.
2. Seleccione con el **click** derecho sobre la carpeta de **Domain Controllers** y del menú contextual seleccione Propiedades. Así las propiedades de **Domain Controllers** se desplegaran.
3. Seleccione el **Group Policy** de las pestañas y seleccione **Domain Controller Policy** de la lista de opciones.
4. Pulse **edit** entonces la consola de **Group Policy** se desplegara.
5. Pulse sobre la opción de **Computer Configuration**.
6. Dentro de la opción de **Windows Settings** aparecerá **Security Settings** y luego **Local Policies** y expanda la opción de **Audit Policy**.
7. Seleccione la opción de auditoria que desea habilitar/deshabilitar dando doble clic y aparecerá el cuadro de dialogo correspondiente a la opción.
8. Seleccione el cuadro de selección de **Success** o **Failure** según la acción que se quiera auditar.
9. Clic en OK.
10. Cierre la consola de **Group Policy**.
11. Por ultimo abra una consola de comandos y escriba el comando **gpupdate** y presione **enter**. Los cambios tomaran efecto en unos pocos minutos.

Administrar registros de seguridad

Herramientas del Administrador de configuración de seguridad

Estas herramientas se pueden utilizar para administrar la directiva de seguridad de un equipo, unidad organizativa o dominio.

Herramienta del Administrador de configuración de seguridad	Descripción
Plantillas de seguridad	Una plantilla de seguridad es un archivo que representa una configuración o una directiva de seguridad. Estas plantillas se pueden aplicar a un equipo local o importarse en un objeto de Directiva de grupo.
Configuración y análisis de seguridad	Puede utilizar esta herramienta para analizar o configurar la seguridad de los equipos, utilizando una plantilla de seguridad.
Extensión Configuración de seguridad para Directiva de grupo	Puede utilizar esta herramienta para modificar la configuración de seguridad individual de un dominio, sitio o unidad organizativa.
Directiva de seguridad local	Puede utilizar esta herramienta para modificar la configuración de seguridad individual del equipo local.
Automatizar las tareas de configuración de la seguridad	Puede utilizar esta herramienta para automatizar tareas de configuración de seguridad.

Para modificar una opción de configuración de seguridad en un objeto de directiva de grupo

Para el equipo local

1. Abra Configuración de seguridad local.
2. En el árbol de la consola, haga clic en **Configuración de seguridad**.
3. Realice una de estas acciones:
   - Para modificar la **Directiva de contraseñas** o la **Directiva de bloqueo de cuentas**, haga clic en **Directivas de cuentas**.
   - Para modificar la **Directiva de auditoría**, la **Asignación de derechos de usuario** o las **Opciones de seguridad**, haga clic en **Directivas locales**.
4. En el panel de detalles, haga doble clic en la opción de configuración que desee modificar.
5. Modifique la opción y, después, haga clic en **Aceptar**.

Para un objeto de directiva de grupo, si está en una estación de trabajo o un servidor que se ha unido a un dominio.

1. En la barra de tareas, haga clic en **Inicio**, seleccione **Ejecutar**, escriba **mmc** y haga clic en **Aceptar**.
2. En la consola, en el menú **Archivo**, haga clic en **Agregar o quitar complemento**.

3. En **Agregar o quitar complemento**, haga clic en **Agregar** y, a continuación, en **Agregar un complemento independiente**, haga doble clic en **Editor de objetos de directiva de grupo.**

4. En **Seleccionar un objeto de directiva de grupo**, haga clic en **Examinar**, busque el objeto de directiva que desee modificar y haga clic en **Finalizar**.
5. Haga clic en **Cerrar** y, después, haga clic en **Aceptar**.

6. En el árbol de la consola, haga clic en **Configuración de seguridad**.

Directiva Objeto de directiva de grupo [nombreDeEquipo]\Configuración del equipo\Configuración de Windows\Configuración de seguridad

Realice una de estas acciones

- Para modificar la **Directiva de contraseñas**, la **Directiva de bloqueo de cuentas** o la **Directiva Kerberos**, en el panel de detalles, haga doble clic en **Directivas de cuentas.**
- Para modificar la **Directiva de auditoría**, la **Asignación de derechos de usuario** o las **Opciones de seguridad**, en el panel de detalles, haga doble clic en **Directivas locales**.
- Para modificar la configuración del registro de sucesos, en el árbol de la consola, haga clic en **Registro de sucesos**.

7. En el panel de detalles, haga doble clic en la opción de configuración de seguridad que desee modificar
8. Modifique la opción y, después, haga clic en **Aceptar**.

Prácticas recomendadas para auditar sucesos de seguridad

- *Crear un plan de auditoría antes de implementar la directiva de auditoría.*

Decida el tipo de información que se desea obtener mediante la recopilación de sucesos de auditoría:

Si está interesado en la detección de intrusos (realizar un seguimiento de los intentos que efectúan los usuarios para obtener acceso a áreas en las que no tienen autorización), puede recopilar auditorías de errores. Pero habilitar las auditorías de errores puede constituir un riesgo para su organización. Si los usuarios intentan tener acceso a un recurso para el que no tienen autorización, puede crear tantas auditorías de errores que el registro de seguridad se llene y el equipo ya no pueda recopilar más auditorías. Si está habilitada la configuración de directiva **Auditoría: apagar el sistema de inmediato si no puede registrar auditorías de seguridad**, los usuarios pueden iniciar un ataque de denegación de servicio a través de la directiva de auditoría.

Si está interesado en utilizar el registro de auditoría para determinar exactamente lo que ha sucedido en la organización, puede recopilar una combinación de auditorías de aciertos y errores.

Considere los recursos que tiene disponibles para recopilar y revisar un registro de auditoría. Los sucesos de auditoría ocupan espacio en los equipos y puede ocupar su tiempo y el de las personas de su organización. No audite los sucesos en los que no esté realmente interesado.

- *Recopilar y archivos registros de seguridad en la organización.*

Si se produce una intrusión, aísle y conserve las entradas del registro de seguridad. Estas entradas pueden resultar valiosas durante la investigación de una intrusión.

Una pista de auditoría puede contener información acerca de los cambios efectuados en su equipo o en otros equipos de la red. Si los intrusos obtienen derechos y permisos de administrador, o si los administradores hacen un uso abusivo de sus derechos y permisos, puede borrar el registro de seguridad, por lo que no dispondría de ninguna pista de sus acciones. Si utiliza una herramienta que recopile y guarde periódicamente las entradas de los registros de seguridad de la organización, incluso si los intrusos o los administradores borran el registro de seguridad local, es muy probable que pueda realizar un seguimiento de las acciones de los intrusos o los administradores. Un ejemplo de este tipo de herramienta es Microsoft Operations Manager.

- *Auditar sucesos de aciertos y errores en la categoría de sucesos del sistema.*

Mediante la auditoría de los sucesos de aciertos y errores en la categoría de sucesos del sistema, puede advertir actividades poco habituales que puedan indicar que un intruso intenta obtener acceso al equipo o a la red.

El número de auditorías que se generan cuando está habilitada esta configuración tiende a ser relativamente bajo y la calidad de la información que se obtiene de los sucesos tiende a ser relativamente alta.

- *Auditar sucesos de aciertos en la categoría de sucesos de cambio de directivas en los controladores de dominio.*

Si se registra un suceso en la categoría de sucesos de cambio de directivas, significa que alguien ha cambiado la configuración de la directiva de seguridad Autoridad de seguridad local (LSA).

Si utiliza Directiva de grupo para editar la configuración de la directiva de auditoría, no es necesario auditar los sucesos en la categoría de sucesos de cambio de directivas en los servidores miembro.

Si decide auditar sucesos de errores en la categoría de sucesos de cambio de directivas, puede ver si usuarios no autorizados o atacantes intentan cambiar la configuración de directivas, incluida la configuración de directivas de seguridad. Aunque puede resultar útil para la detección de intrusos, el aumento en recursos necesarios y la posibilidad de un ataque de denegación de servicio normalmente no compensan las ventajas.

- *Auditar sucesos de aciertos en la categoría de sucesos de administración de cuentas.*

Mediante la auditoría de sucesos de aciertos en la categoría de sucesos de administración de cuentas, puede comprobar los cambios que se realizan en las propiedades de cuentas y de grupos.

Si decide auditar sucesos de errores en la categoría de sucesos de administración de cuentas, puede ver si usuarios no autorizados o atacantes intentan cambiar las propiedades de cuentas o grupos. Aunque puede resultar útil para la detección de intrusos, el aumento en recursos necesarios y la posibilidad de un ataque de denegación de servicio normalmente no compensan las ventajas.

- *Auditar sucesos de aciertos en la categoría de sucesos de inicio de sesión.*

Mediante la auditoría de sucesos de aciertos en la categoría de sucesos de inicio de sesión, dispondrá de un registro de cuándo los usuarios inician o cierran la sesión en un equipo. Si un usuario no autorizado roba la contraseña de otro usuario e inicia sesión en un equipo, puede determinar cuándo se produjo la infracción de seguridad.

Si decide auditar sucesos de errores en la categoría de sucesos de inicio de sesión, puede ver si usuarios no autorizados o atacantes intentan iniciar sesión en un equipo. Aunque puede resultar útil para la detección de intrusos, la posibilidad de un ataque de denegación de servicio aumenta con la auditoría de sucesos de errores en la categoría de sucesos de inicio de sesión. Si la auditoría de errores está habilitada en estas categorías de sucesos, los usuarios que no pertenezcan a su organización podrían llenar el registro de seguridad o provocar que se sobreescriban los sucesos mediante el intento continuo de iniciar una sesión en la red con nombres de usuario o contraseñas incorrectos. Si además está habilitada la configuración de directiva **Auditoría: apagar el sistema de inmediato si no puede registrar auditorías de seguridad**, las consecuencias del registro de los sucesos de errores en estas categorías pueden ser aún más graves: el usuario podría causar una denegación de servicio si se llena el registro de seguridad.

- *Auditar sucesos de aciertos en la categoría de sucesos de inicio de sesión de cuenta en los controladores de dominio.*

Mediante la auditoría de sucesos de aciertos en la categoría de sucesos de inicio de sesión de cuenta, puede ver cuándo los usuarios inician o cierran la sesión en el dominio.

No es necesario auditar sucesos en la categoría de sucesos de inicio de sesión en los servidores miembro.

Si decide auditar sucesos de errores en la categoría de sucesos de inicio de sesión de cuenta, puede ver si usuarios no autorizados o atacantes intentan iniciar sesión en la red. Aunque puede resultar útil para la detección de intrusos, la posibilidad de un ataque de denegación de servicio aumenta con la auditoría de sucesos de errores en la categoría de sucesos de inicio de sesión de cuenta. Si la auditoría de errores está habilitada en estas categorías de sucesos, los usuarios que no pertenezcan a su organización podrían llenar el registro de seguridad o provocar que se sobreescriban los sucesos mediante el intento

continuo de iniciar una sesión en la red con nombres de usuario o contraseñas incorrectos. Si además está habilitada la configuración de directiva **Auditoría: apagar el sistema de inmediato si no puede registrar auditorías de seguridad**, las consecuencias del registro de los sucesos de errores en estas categorías pueden ser aún más graves: el usuario podría causar una denegación de servicio si se llena el registro de seguridad.

- *Configurar de forma específica la auditoría en un objeto.*

Para auditar el acceso a objetos, debe habilitar la configuración de directiva **Auditar el acceso a objetos** y, a continuación, editar la lista de control de accesos del sistema (SACL) que está asociada al objeto.

Para conseguir el máximo rendimiento, minimice el número de entradas en la SACL para un objeto. Una entrada en una SACL que contenga 1000 usuarios no degrada el rendimiento del sistema como lo harían 1000 entradas independientes.

Para reducir el volumen de sucesos que se generan y para maximizar la eficacia de cada suceso, audite únicamente las acciones en las que realmente esté interesado. Por ejemplo, si está interesado en los usuarios que leen un archivo, no audite Control total.

- *Configurar un tamaño adecuado para el registro de seguridad.*

Es importante que el tamaño del registro de seguridad se configure correctamente, según el número de sucesos que genera la configuración de directiva de auditoría.

Tamaño máximo del registro de seguridad

Esta opción de configuración de seguridad indica el tamaño máximo del registro de sucesos de seguridad, cuyo límite superior es de 4 GB.

El tamaño de los archivos de registro debe ser un múltiplo de 64 KB. Si se especifica un valor que no es múltiplo de 64 KB, el Visor de sucesos establecerá el tamaño del archivo de registro a un múltiplo de 64 KB.

Esta opción no aparece en el objeto de directiva de equipo local.

El tamaño del registro de sucesos y el ajuste de registro deben definirse de forma que coincidan con los requisitos empresariales y de seguridad que se especificaron al diseñar el plan de seguridad empresarial. Procure implementar estos valores de configuración del registro de sucesos por sitios, dominios y unidades organizativas para aprovechar así la configuración de la directiva de grupo.