

Configuración de servidores con Linux/Unix y Windows NT/2K/XP

Tabla de Contenidos

4. Configuración de servidores con Linux/Unix y Windows NT/2K/XP.....	2
4.1 Compartir recursos desde Windows NT/2K/XP.....	2
4.1.1 El directorio activo.....	3
4.1.2 Creación de cuentas de usuario.....	3
4.1.2.1 Creación de cuentas de usuario del dominio.....	4
4.1.2.2 Creación de cuentas de usuario locales.....	6
4.1.3 Administración de las cuentas de usuario.....	6
4.1.4 Perfiles de usuario.....	9
4.1.4.1 Perfiles locales.....	10
4.1.4.2 Perfiles móviles.....	10
4.1.4.3 Perfiles obligatorios.....	11
4.1.5 Recursos compartidos y permisos.....	12
4.1.5.1 Permisos en NTFS frente a FAT.....	12
4.1.5.2 Recursos compartidos especiales.....	13
4.1.5.3 4.1.5.3-Carpetas compartidas.....	14
4.1.5.4 Creación de un nuevo recurso compartido para una carpeta compartida.....	15
4.1.5.5 Desconexión de carpetas compartidas.....	16
4.1.5.6 Permisos de recursos compartidos.....	16
4.1.5.7 Definición de los permisos de recursos compartidos.....	16
4.1.5.8 Permisos de recursos compartidos.....	17
4.1.5.9 Definición de los permisos de recursos compartidos.....	17
4.1.5.10 Asignación de directorios y unidades compartidas.....	18
4.1.5.11 Desconexión de recursos conectados.....	19
4.1.5.12 Permisos para carpetas y archivos.....	19
4.1.5.13 Funcionamiento de los permisos.....	20
4.1.5.14 Configuración de los permisos de las carpetas.....	20
4.1.5.15 Asignación de permisos a los archivos.....	21
4.1.5.16 Configuración de permisos especiales.....	21
4.2 Compartir recursos desde Linux/Unix.....	23
4.2.1 SMB (Samba).....	23
4.2.1.1 Sección [global].....	24
4.2.1.2 Sección [homes].....	25
4.2.1.3 Sección [printers].....	25
4.2.1.4 Seguridad en SAMBA.....	26
4.2.2 NFS (Network File System).....	29



4. Configuración de servidores con Linux/Unix y Windows NT/2K/XP

4.1 Compartir Recursos Desde Windows NT/2K/XP

Vamos a tomar como base para las explicaciones teoricas de estos dos capitulos la version Windows 2000, debido a que actualmente es la mas implantada en empresas, por encima de otras como NT, o 2003.

Si se desea crear una red bajo windows 2000 y compartir los diferentes recursos que en ella tengamos deberemos hacerlo de una de dos maneras:

- **En un grupo de trabajo (*workgroup*).** Un grupo de trabajo es una agrupación lógica de máquinas, sin ningún otro fin. Los ordenadores que forman parte del mismo grupo aparecen juntos cuando se explora el "Entorno de Red" (o red de ordenadores NetBIOS). En este caso, la administración de cada ordenador es local e independiente del resto. Para poder acceder a los recursos que exporta un ordenador concreto, el usuario remoto tiene que disponer necesariamente de
- **Formando parte de un dominio (*domain*).** se puede definir *dominio* como una agrupación lógica de servidores de red y otros ordenadores, que comparten información común sobre cuentas (de usuarios, grupos, equipos, etc.) y seguridad. Mediante un dominio es la forma en que se recomienda que se defina una red de máquinas Windows 2000. En el, la información administrativa se encuentra *centralizada*, y por ello resulta más fácil y segura de gestionar.

Para la creacion de un dominio bajo Windows 2000 es necesaria la existencia de un controlador de dominio como minimo, o domain controler (DC), o de varios que administraran la informacion de manera conjunta y repartiran la carga dentro de un mismo nivel de jerarquia. Pueden existir servidores miembro sin ser controladores de dominio. Estos servidores se encargaran de facilitar servicios especificos dentro del sominio (impresion , servidores web,etc.). Un dominio bajo windows 2000 podra existir de dos formas:

- **Modo mixto:** Utilizado en el caso en el que algunos controladores del dominio funcionan bajo Windows NT y otros bajo Windows 2000., compartiendo informacion administrativa.
- **Modo nativo:** Todos los DC funcionan bajo Windows 2000. Esto permite utilizar funcionalidades especificamente diseñadas para este sistema operativo, tales como el directorio activo.



4.1.1 El Directorio Activo

El Directorio Activo es un servicio de red que almacena información acerca de los recursos existentes en la red y controla el acceso de los usuarios y las aplicaciones a dichos recursos. De esta forma, se convierte en un medio de organizar, administrar y controlar centralizadamente el acceso a los recursos de la red.

El Directorio Activo se ha implementado siguiendo una serie de estándares y protocolos existentes, ofreciendo interfaces de programación de aplicaciones que facilitan la comunicación con otros servicios de directorio. Entre ellos, se pueden encontrar los siguientes:

- DHCP (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de ordenadores, que permite la administración desatendida de direcciones de red.
- DNS (Domain Name System). Servicio de nombres de dominio que permite la administración de los nombres de ordenadores. Este servicio constituye el mecanismo de asignación y resolución de nombres (traducción de nombres simbólicos a direcciones IP) en Internet.
- SNTP (Simple Network Time Protocol). Protocolo simple de tiempo de red, que permite disponer de un servicio de tiempo distribuido.
- LDAP (Lightweight Directory Access Protocol). Protocolo ligero (o compacto) de acceso a directorio. Este es el protocolo mediante el cual las aplicaciones acceden y modifican la información existente en el directorio.
- Kerberos V5. Protocolo utilizado para la autenticación de usuarios y máquinas..
- Certificados X.509. Estándar que permite distribuir información a través de la red de una forma segura.

4.1.2 Creacion De Cuentas De Usuario

Windows 2000 sólo crea dos cuentas predefinidas: la cuenta *Administrador*, que otorga al usuario todos los derechos y permisos, y la cuenta *Invitado*, que tiene derechos limitados. El resto de las cuentas las crea un administrador y son cuentas de dominio (válidas a lo largo de todo el dominio de forma predeterminada) o cuentas locales (utilizables sólo en la máquina donde se crean).

La planificación de las opciones de las cuentas de los usuarios simplificará el proceso de creación de cuentas. Las opciones de las cuentas a considerar incluyen las siguientes:

- **Horas de inicio de sesión:** De forma predeterminada, un usuario puede iniciar sesión a cualquier hora del día o de la noche. Por razones de seguridad, se podría restringir el acceso a algunos o a todos los usuarios a ciertas horas del día o a ciertos días de la semana.
- **Iniciar sesión en:** De forma predeterminada, los usuarios pueden iniciar sesión en todas las estaciones de trabajo. Por razones de seguridad se puede limitar el acceso para iniciar sesión a una máquina o máquinas en particular si se dispone del protocolo NetBIOS instalado en el dominio. Sin NetBIOS, Windows 2000 es incapaz de determinar la ubicación de un inicio de sesión específico.
- **Caducidad de la cuenta:** Se puede decidir si se desea establecer que las cuentas caduquen. Por razones obvias, tiene sentido establecer una fecha de caducidad para empleados temporales de forma que coincida con el fin de sus contratos.

Las tres opciones que se han enumerado aquí son las que muy posiblemente se apliquen a un gran número de usuarios.

4.1.2.1 Creación De Cuentas De Usuario Del Dominio

Las cuentas de usuario del dominio se pueden crear en el contenedor Users o en algún otro contenedor u OU creada para almacenar cuentas de usuario del dominio. Para añadir una cuenta de usuario del dominio hay que seguir estos pasos:

- Abrir **Usuarios y equipos de Active Directory** desde el menú **Herramientas administrativas**.
- Resaltar el nombre del dominio y, en el menú **Acción**, apuntar a **Nuevo** y escoger después **Usuario**.
- **Nombre, Iniciales y Apellidos:** Un nombre de usuario no puede coincidir con otro nombre de usuario o de grupo en el equipo que está administrando. Puede contener hasta 20 caracteres, en mayúsculas o minúsculas, excepto los siguientes: " / [] : ; | = , + * ? < >
- **Nombre completo:** se rellena automáticamente. El nombre completo debe ser único en la OU donde se crea el usuario.

- **Nombre de inicio de sesión de usuario:** Hay que proporcionar el nombre de inicio de sesión de usuario basado en un convenio de denominación que previamente se ha tenido que establecer. Este nombre debe ser único en el Active Directory. El nombre de inicio de sesión anterior a Windows 2000 se rellena automáticamente. Este es el nombre utilizado para iniciar sesión desde equipos que ejecutan sistemas operativos Windows como Windows NT. Pulsar **Siguiente**.
- **Contraseña y Confirmar contraseña:** Se puede escribir una contraseña que contenga hasta 127 caracteres. Sin embargo, si utiliza Windows 2000 en una red que también contiene equipos con Windows 95 ó Windows 98, considere el uso de contraseñas con menos de 14 caracteres. Windows 95 y Windows 98 admiten contraseñas de hasta 14 caracteres. Si la contraseña es más larga no se podrá iniciar sesión en la red desde estos equipos.
Todos los usuarios deberían tener contraseñas bien escogidas y se les debería requerir que las cambiaran periódicamente. Las cuentas deberían establecerse de forma que se bloquearan cuando se introdujeran contraseñas incorrectas. (Se pueden permitir tres intentos, para dejar margen a errores tipográficos).

Los administradores deberían tener dos cuentas en el sistema: una cuenta administrativa y una cuenta de usuario normal. Se debería utilizar la cuenta de usuario normal a menos que se estén realizando tareas administrativas. A causa de los privilegios asociados a las cuentas administrativas, son un objetivo primario para los intrusos.

Directivas de contraseñas:

- **El usuario debe cambiar la contraseña en el siguiente inicio de sesión:** Normalmente se selecciona para que el usuario controle la contraseña y no la conozca el Usuario que le ha dado de alta.
- **El usuario no puede cambiar la contraseña:** Cuando por necesidades de seguridad la contraseña debe ser controlada por el administrador.
- **La contraseña nunca caduca:** Si seleccionamos esta casilla, no se aplicarán las restricciones de caducidad de contraseña a esta cuenta.
- **Cuenta deshabilitada:** Deshabilita cuentas que momentáneamente no se necesitan en la red. También puede seleccionarse automáticamente debido a las restricciones de seguridad impuestas por el Administrador. Pulsar **Siguiente**.

Se abre una pantalla de confirmación, mostrando los detalles de la cuenta que se va a crear. Si los detalles son correctos, hay que pulsar **Finalizar**. En otro caso, se puede utilizar el botón **Atrás** para realizar correcciones.



4.1.2.2 Creación De Cuentas De Usuario Locales

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

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

4.1.3 Administración De Las Cuentas De Usuario

Abrir **Usuarios y equipos de Active Directory** desde el menú **Herramientas administrativas**. Abrir el contenedor que almacena la cuenta de usuario. **Seleccionar el Usuario** que queremos administrar y pulsar el menú **Acción**. Aparecerán las siguientes opciones:

Copiar:

- Escriba el nombre del usuario en **Nombre**.
- En **Apellidos**, escriba los apellidos.
- Modifique **Nombre** para agregar iniciales o invertir el orden del nombre y los apellidos.
- En **Nombre de inicio de sesión de usuario**, escriba el nombre con el que el usuario iniciará una sesión y, en la lista, haga clic en el sufijo UPN que se debe anexar al nombre de inicio de sesión de usuario, seguido del símbolo arroba (@).

Si el usuario va a utilizar un nombre diferente para iniciar una sesión en equipos donde se ejecuta Windows

NT, Windows 98 o Windows 95, cambie el nombre de inicio de sesión de usuario que aparece en **Nombre de inicio de sesión de usuario (anterior a Windows 2000)** por el otro nombre.

En **Contraseña y Confirmar contraseña**, escriba la contraseña del usuario.

- Seleccione las opciones de contraseña que desee.
- Si se ha deshabilitado la cuenta de usuario desde la que se copió la nueva cuenta de usuario, haga clic en **Cuenta deshabilitada** para habilitar la cuenta nueva.

Agregar miembros a un grupo

Si queremos hacer miembro de otro grupo más al usuario deberemos pulsar esta opción y seleccionar el grupo y después **Agregar**.

Deshabilitar cuenta

Si es necesario desactivar una cuenta de usuario del dominio por algún periodo de tiempo, pero no eliminarla permanentemente, se puede deshabilitar. Si crea cuentas deshabilitadas de usuario que pertenezcan a grupos comunes, puede utilizarlas como plantillas para simplificar la creación de cuentas de usuario. Para **habilitar** una cuenta previamente deshabilitada, hay que realizar los mismos pasos, escogiendo **Habilitar cuenta** en el menú contextual.

Restablecer contraseña

Para que las contraseñas sean efectivas, no deben ser obvias o fáciles de adivinar. Sin embargo, cuando las contraseñas no sean obvias o fáciles de adivinar, se olvidaran inevitablemente. Cuando un usuario olvida su contraseña, se puede restablecer. La mejor política es restablecerla a una clave sencilla y obligar al usuario a que la cambie la próxima vez que inicie sesión en la red.

- Hay que escribir y confirmar la contraseña.
- Si desea que el usuario cambie esta contraseña en el siguiente proceso de inicio de sesión, active la casilla de verificación **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**.
- Si se cambia la contraseña de la cuenta de usuario de un servicio, deben restablecerse todos los servicios cuya autenticación se realice con esa cuenta de usuario.



Mover

Si un usuario pasa a pertenecer a otro grupo o Unidad Organizativa podemos moverlo pulsando esta opción. En el cuadro de diálogo Mover, hay que resaltar el contenedor destino y pulsar **Aceptar**.

Abrir la página principal

Accederemos a la página web del usuario si se le ha especificado en la ficha General de las propiedades de dicho usuario.

Enviar mensaje de correo

Si se le ha especificado una dirección de correo, se abrirá el cliente de correo predeterminado para enviarle un correo electrónico.

Eliminar

Cada cuenta de usuario del dominio tiene un identificador de seguridad asociado que es único y nunca se reutiliza, lo que significa que una cuenta eliminada se elimina completamente. Si se elimina la cuenta de Jaime y más tarde se cambia de opción, habrá que volver a crear no sólo la cuenta, sino los permisos, la configuración, las pertenencias a grupos y el resto de propiedades que poseía la cuenta de usuario original. Por esta razón, si existe alguna duda sobre si una cuenta podría necesitarse en el futuro, es mejor deshabilitarla y no realizar la eliminación hasta que se este seguro de que no se necesitará de nuevo.

Después de pulsar en eliminar, aparece un cuadro de diálogo Active Directory, pidiendo confirmación de la eliminación. Hay que pulsar Si y se eliminará la cuenta.

Cambiar el nombre

En ocasiones, es necesario cambiar el nombre de una cuenta de usuario. Por ejemplo, si se tiene una cuenta configurada con una colección de derechos, permisos y pertenencias a grupos para una posición particular y una nueva persona se hace cargo de esa posición se puede cambiar el nombre, los apellidos y el nombre de inicio de sesión de usuario para la nueva persona.

Para cambiar el nombre de una cuenta de usuario existente, después de pulsar el cambiar el nombre se pulsa **Aceptar**. Se cambia el nombre de la cuenta y todos los permisos y el resto de la configuración permanecen intactos. Si queremos cambiar alguna información más, habrá que entrar en la ficha de Propiedades del usuario.

Actualizar

Produce un refresco de la pantalla



Propiedades

La ventana Propiedades de un usuario del dominio puede tener hasta una docena de pestañas, dependiendo de la configuración del dominio. Toda la información introducida en la ventana Propiedades se puede utilizar como la base de una búsqueda en el Active Directory.

4.1.4 Perfiles De Usuario

Un perfil es un entorno personalizado específicamente para un usuario. El perfil contiene la configuración de escritorio y de los programas del usuario. Cada usuario tiene un perfil, tanto si el administrador lo configura como si no, porque se crea un perfil automáticamente para cada usuario cuando inicia sesión en un equipo. Los perfiles ofrecen numerosas ventajas:

- Múltiples usuarios pueden utilizar el mismo equipo, con la configuración de cada uno recuperada al iniciar la sesión al mismo estado en que estaba cuando cerró la sesión.
- Los cambios hechos por un usuario en el escritorio no afectan a otro usuario.
- Si los perfiles de usuario se almacenan en un servidor pueden seguir a los usuarios a cualquier equipo de la red que ejecute Windows 2000 o Windows NT 4.

Desde el punto de vista de un administrador, la información del perfil puede ser una valiosa herramienta para configurar perfiles de usuario predeterminados para todos los usuarios de la red o para personalizar los perfiles predeterminados para diferentes departamentos o clasificaciones del trabajo. También se pueden configurar perfiles obligatorios que permitan a un usuario hacer cambios en el escritorio mientras esta conectado, pero no guardar ninguno de los cambios. Un perfil obligatorio siempre se muestra exactamente igual cada vez que un usuario inicia sesión. Los tipos de perfiles son los siguientes:

- **Perfiles locales:** Perfiles creados en un equipo cuando un usuario inicia sesión. El perfil es específico de un usuario, local al equipo y se almacena en el disco duro del equipo local.
- **Perfiles móviles:** Perfiles creados por un administrador y almacenados en un servidor. Estos perfiles siguen al usuario a cualquier máquina Windows 2000 o Windows NT 4 de la red.
- **Perfiles obligatorios:** Perfiles móviles que sólo pueden ser modificados por un administrador.

4.1.4.1 Perfiles Locales

Los perfiles locales se crean en los equipos cuando los usuarios individuales inician sesión. En un equipo actualizado desde Windows NT 4, el perfil se almacena en la carpeta Perfiles de la partición raíz del sistema. En un equipo con una nueva instalación de Windows 2000, el perfil del usuario está en la carpeta Documents and Settings.

La primera vez que un usuario inicia sesión en un equipo, se genera una carpeta de perfil para el usuario, y los contenidos de la carpeta Default User se copian en ella. Cualquier cambio realizado por el usuario al escritorio se almacena en ese perfil de usuario cuando cierra la sesión.

Si un usuario tiene una cuenta local en el equipo además de una cuenta de dominio a inicia sesión varias veces utilizando ambas cuentas, el usuario tendrá dos carpetas de perfil en el equipo local: una para cuando el usuario inicie sesión en el dominio utilizando la cuenta de usuario del dominio y otra para cuando el usuario inicie sesión localmente en el equipo. El perfil local se mostrará con el nombre de inicio de sesión. El perfil de dominio también se mostrará con el nombre de inicio de sesión, pero llevará añadido el nombre del dominio.

4.1.4.2 Perfiles Móviles

Los perfiles móviles son una gran ventaja para los usuarios que utilizan frecuentemente más de un equipo. Un perfil móvil se almacena en un servidor y, después de que el inicio de sesión del usuario sea autenticado en el servicio de directorio, se copia al equipo local. Esto permite al usuario tener el mismo escritorio, la configuración de las aplicaciones y la configuración local en cualquier máquina que ejecute Windows 2000 o Windows NT 4.

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

Cuando el usuario inicia sesión de nuevo, el perfil del servidor se compara con la copia en el equipo local y se carga para el usuario la más reciente. Si el servidor no está disponible, se utiliza la copia local. Si el servidor no está disponible y es la primera vez que el usuario ha iniciado sesión en el equipo, se crea un perfil de usuario localmente

utilizando el perfil Default User. Cuando un perfil no es descargado a un equipo local a causa de problemas con el servidor, el perfil móvil no se actualiza cuando el usuario cierra la sesión.

Configuración de los perfiles móviles

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

1. Crear una carpeta compartida en el servidor para los perfiles.

2. En la pestaña Perfil de la ventana Propiedades de la

cuenta de usuario hay que proporcionar una ruta de acceso a la carpeta compartida, como \\nombre_del_servidor\carpeta_de_perfiles_compartida\%username%.

Una vez que se ha creado una carpeta de perfiles compartida en un servidor y se ha suministrado una ruta de acceso al perfil en la cuenta del usuario, se ha habilitado un perfil móvil. La configuración del usuario de su escritorio se copia y almacena en el servidor y estará disponible para el usuario desde cualquier equipo.

4.1.4.3 Perfiles Obligatorios

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



4.1.5 Recursos Compartidos Y Permisos

El objetivo principal de una red es compartir recursos entre los usuarios. Sin embargo, compartir es también una extensión de las características de seguridad que comienzan con las cuentas de usuario y las contraseñas. El objetivo como administrador del sistema es asegurarse de que todo el mundo pueda utilizar los recursos que necesita sin comprometer la seguridad de los archivos y el resto de los recursos. Se pueden otorgar a los usuarios tres tipos de capacidades:

- **Derechos:** están asignados a los grupos predefinidos, pero el administrador puede extender los derechos a grupos o individuos.
- **Recursos compartidos:** Directorios o unidades de disco que están compartidos en la red.
- **Permisos:** Capacidades del sistema de archivos que se pueden conceder tanto a individuos como a grupos.

4.1.5.1 Permisos En NTFS Frente A FAT

En un volumen NTFS, Windows 2000, al igual que Windows NT Server, permite una seguridad tan granular que es prácticamente microscópica. Se pueden establecer permisos de varios tipos, incluyendo permisos en archivos individuales. Esto representa realmente una tentación para el administrador para gestionar al detalle cada recurso. El mejor consejo que se puede dar es no caer en esta tentación. Se debe comenzar con la menor restricción posible y añadir restricciones solo cuando se requieran.

En particiones con formato FAT se pueden restringir los archivos solo a nivel de carpeta, sólo desde la red y sólo si la carpeta esta compartida. Para alguien que inicie sesión localmente, los recursos compartidos no tendrán efecto.

En un volumen NTFS, los directorios pueden ser compartidos y también restringidos más profundamente a causa del significado de los permisos. En un volumen NTFS, se deberían utilizar los permisos de carpetas y archivos para el control de la seguridad tanto localmente como desde la red y permitir acceso de Control total a Todos en el recurso compartido.



Para determinar los permisos reales de acceso a un recurso se siguen los siguientes pasos:

1. **Determinar el permiso de compartición (FAT) efectivo.** El permiso de compartición (FAT) efectivo será el permiso más restrictivo de todos aquéllos asignado a un usuario o a los grupos a los que el usuario pertenece. La excepción es el de Denegar Control Total que anulará el resto de permisos.
2. **Determinar el permiso de NTFS efectivo.** El permiso de NTFS efectivo será el más permisivo de todos los permisos de NTFS asignados al usuario y a los grupos a los que el usuario pertenece. La excepción es que si existe Sin Acceso, se niegan el resto de los permisos asignados
3. **El permiso global efectivo será el más restrictivo entre el permiso efectivo de compartición (FAT) y el permiso efectivo de NTFS.** El permiso de compartición (FAT) sería de control total para Luis. El permiso NTFS efectivo para Luis sería Sin Acceso (Denegar Control Total es el equivalente a Sin Acceso). El más restrictivos entre Control Total y Sin Acceso será Sin Acceso que es el permiso efectivo de acceso de Luis al recurso.

4.1.5.2 Recursos Compartidos Especiales

Además de los recursos compartidos creados por un usuario o un administrador, el sistema crea varios recursos compartidos especiales que no se deberían modificar o eliminar. El recurso compartido especial que más probablemente se verá es el recurso compartido ADMIN\$ que aparece como C\$, D\$, E\$, etc. Estos recursos compartidos permiten a los administradores conectarse a unidades que en otro caso no estarían compartidas.

Los recursos compartidos especiales existen como parte de la instalación del sistema operativo. Dependiendo de la configuración del equipo, estarán presentes algunos o todos de los siguientes recursos compartidos especiales. Ninguno de ellos debería modificarse o eliminarse.

- **ADMIN\$:** Se utiliza durante la administración remota de un equipo. La ruta de acceso es siempre la ubicación de la carpeta en la que Windows se instaló (esto es, la raíz del sistema). Solo los Administradores, Operadores de copia y Operadores de servidores se pueden conectar a este recurso compartido.
- **letraunidad\$:** La carpeta raíz de la unidad especificada. Sólo los Administradores, Operadores de copia y Operadores de servidores se pueden conectar a estos recursos compartidos en un servidor Windows 2000. En un equipo Windows 2000 Professional, sólo los Administradores y Operadores de copia pueden conectarse a estos recursos compartidos.

- **IPC\$:** Utilizado durante la administración remota y cuando se revisan los recursos compartidos. Este recurso compartido es esencial en la comunicación y no se debe cambiar, modificar o eliminar.
- **NETLOGON:** Lo utiliza el servicio Inicio de sesión de red de un servidor que ejecuta Windows NT Server cuando procesa los inicios de sesión en el dominio. Este recurso solo se proporciona en servidores, no en Windows NT Workstation.
- **PRINT\$:** Un recurso que soporta impresoras compartidas.
- **REPL\$:** Se crea en un servidor cuando un cliente de fax esta enviando un fax.

Para conectarse a una unidad de disco no compartida en otro equipo, hay que utilizar la barra de direcciones de cualquier ventana a introducir la dirección, utilizando la sintaxis:

```
\\nombre_equipo\[letraunidad]$
```

Para conectarse a la carpeta raíz del sistema (la carpeta en la cual esta instalado Windows) en otro equipo hay que utilizar la sintaxis:

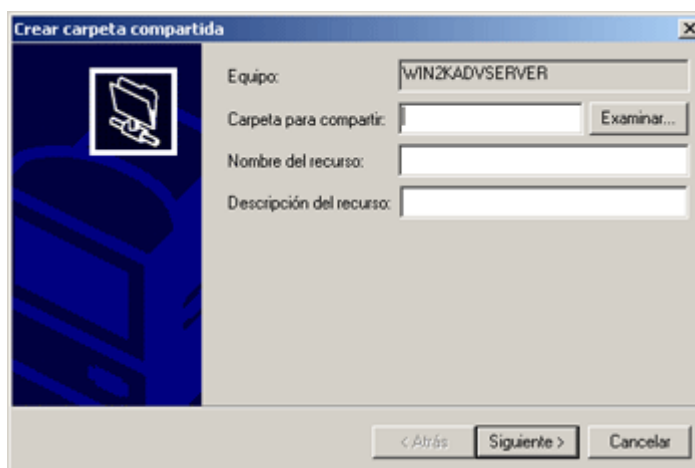
```
\\nombre_equipo\admin$
```

El resto de recursos compartidos especiales como IPC\$ y PRINT\$ los crea y utiliza únicamente el sistema. NETLOGON es un recurso compartido especial en servidores Windows 2000 y Windows NT y se utiliza cuando se procesan peticiones de inicio de sesión en el dominio.

4.1.5.3 Carpetas Compartidas

La forma más sencilla de crear carpetas compartidas es utilizar la herramienta Configurar el servidor del menú Herramientas administrativas. Para hacerlo, hay que seguir estos pasos:

1. Abrir **Configurar el servidor** y pulsar **Servidor de archivos** en la columna de la izquierda.
2. Pulsar el vinculo **Iniciar el Asistente para carpetas compartidas** para abrir el cuadro de dialogo Crear carpeta compartida.
3. Introducir el **nombre y ruta de acceso** de la carpeta y un nombre del recurso compartido.



4. **Seleccionar los permisos** de recurso compartido que se desean asignar a la carpeta teniendo en cuenta que casi siempre es mejor controlar el acceso por medio de permisos en lugar que con recursos compartidos. Pulsar **Finalizar** cuando se haya terminado.

Se pueden definir recursos compartidos directamente pulsando con el botón derecho del ratón en una carpeta, escogiendo Propiedades en el menú contextual y pulsando después en la pestaña Compartir.

4.1.5.4 Creación De Un Nuevo Recurso Compartido Para Una Carpeta Compartida

Una única carpeta puede ser compartida más de una vez. Por ejemplo, un recurso compartido podría incluir Control total para Administradores y otro recurso compartido para usuarios podría ser más restrictivo. Para añadir un nuevo recurso compartido, hay que seguir estos pasos:

1. **Buscar la carpeta compartida** en el Explorador de Windows y pulsar con el **botón derecho del ratón** en ella. Hay que escoger **Compartir** en el menú contextual.
2. En el cuadro de dialogo que se abre, hay que pulsar el botón **Nuevo recurso compartido**.
3. En el cuadro de dialogo Nuevo recurso compartido hay que **introducir un nuevo Nombre de recurso compartido**. (Cada recurso compartido debe tener un nombre único.) Hay que establecer un limite de usuarios, si es necesario.

4. Pulsar **Permisos** para restringir el acceso. De nuevo, de forma predeterminada, la carpeta compartida otorga Control total a todos los usuarios.

4.1.5.5 Desconexión De Carpetas Compartidas

Para que una carpeta deje de estar compartida, hay que abrir Administración de equipos desde el menú Herramientas administrativas. Hay que expandir Herramientas del sistema, después Carpetas compartidas y por ultimo Recursos compartidos. Hay que pulsar con el botón derecho del ratón en la carpeta compartida en el panel de detalles y escoger Dejar de compartir en el menú contextual.

4.1.5.6 Permisos De Recursos Compartidos

Los permisos de recursos compartidos establecen el máximo ámbito de acceso disponible. Otras asignaciones de permisos (en un volumen NTFS) pueden ser más restrictivas, pero no pueden expandirse más allá de los límites establecidos por los permisos de recurso compartido.

4.1.5.7 Definición De Los Permisos De Recursos Compartidos

Para establecer permisos de recursos compartidos, hay que pulsar con el botón derecho del ratón en la carpeta y escoger Compartir en el menú contextual. Hay que pulsar el botón Permisos para abrir el cuadro de diálogo. El tipo de acceso se establece por medio de la lista de la parte inferior. Se pueden utilizar los botones Agregar y Quitar para cambiar quien accede. Los permisos de recursos compartidos se pueden asignar a usuarios individuales, a grupos y a las entidades especiales Todos, SYSTEM, INTERACTIVE, NETWORK y Usuarios autenticados.



Los tipos de permisos de recursos compartidos desde el menos al más restrictivo son:

- **Leer:** Permite ver los nombres de los archivos y subcarpetas, siempre se puede revisar y borrar el registro de seguridad.
- **Modificar:** Permite el acceso de Leer además de permitir agregar archivos y subdirectorios a la carpeta compartida, modificar la información de los archivos y eliminar archivos y subdirectorios.
- **Control total:** Permite todo el acceso de Modificar además de permitir cambiar permisos (sólo en volúmenes NTFS) y tomar posesión (sólo en volúmenes NTFS).

4.1.5.8 Permisos De Recursos Compartidos

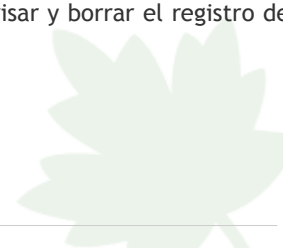
Los permisos de recursos compartidos establecen el máximo ámbito de acceso disponible. Otras asignaciones de permisos (en un volumen NTFS) pueden ser más restrictivas, pero no pueden expandirse más allá de los límites establecidos por los permisos de recurso compartido.

4.1.5.9 Definición De Los Permisos De Recursos Compartidos

Para establecer permisos de recursos compartidos, hay que pulsar con el botón derecho del ratón en la carpeta y escoger Compartir en el menú contextual. Hay que pulsar el botón Permisos para abrir el cuadro de diálogo. El tipo de acceso se establece por medio de la lista de la parte inferior. Se pueden utilizar los botones Agregar y Quitar para cambiar quien accede. Los permisos de recursos compartidos se pueden asignar a usuarios individuales, a grupos y a las entidades especiales Todos, SYSTEM, INTERACTIVE, NETWORK y Usuarios autenticados.

Los tipos de permisos de recursos compartidos desde el menos al más restrictivo son:

- **Leer:** Permite ver los nombres de los archivos y subcarpetas, siempre se puede revisar y borrar el registro de seguridad.



- **Modificar:** Permite el acceso de Leer además de permitir agregar archivos y subdirectorios a la carpeta compartida, modificar la información de los archivos y eliminar archivos y subdirectorios.
- **Control total:** Permite todo el acceso de Modificar además de permitir cambiar permisos (sólo en volúmenes NTFS) y tomar posesión (sólo en volúmenes NTFS).

4.1.5.10 Asignación De Directorios Y Unidades Compartidas

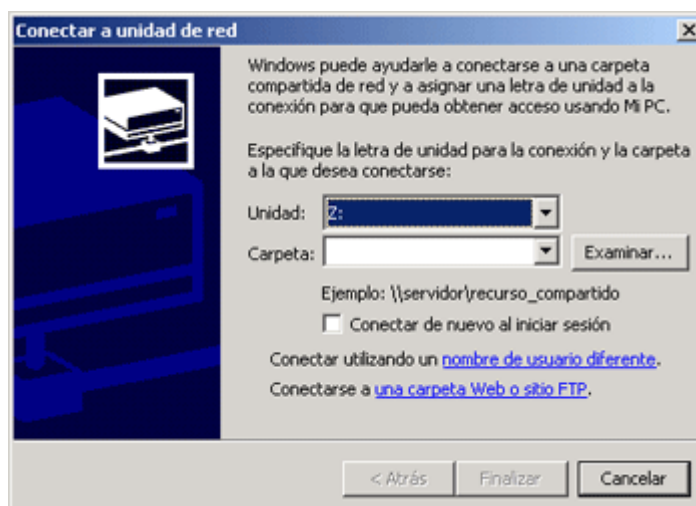
Después de ir de acá para allá entre varias ventanas de Mis sitios de red para buscar una carpeta compartida, los usuarios pueden simplemente pulsar, dos veces con el ratón en la carpeta para abrirla y acceder a su contenido. Para facilitar el acceso, hay que pulsar con el botón derecho del ratón en la carpeta compartida y arrastrarla al escritorio. Hay que seleccionar Crear iconos de acceso directo aquí después de soltar el botón.

Si se utiliza frecuentemente, es sencillo conectarse a una carpeta o unidad de disco para que aparezca en el Explorador de Windows (o en Mi PC) como otra simple unidad de disco local.

Para configurar estas conexiones para los usuarios deberemos seleccionar **Mis sitios de red** y pulsar con el botón derecho del ratón para que aparezca el menú contextual y seleccionar **Conectar a unidad de red**. El cuadro de diálogo que aparece tiene tres entradas configurables:

- **Unidad:** Esta es la letra que se asignara a la nueva carpeta o unidad en el equipo local.
- **Carpeta:** Ruta hasta el recurso compartido
- **Conectar utilizando un nombre de usuario diferente:** Si la conexión es para alguien distinto del usuario actual, hay que pulsar este vínculo y suministrar el nombre y contraseña del usuario.
- **Conectar de nuevo al iniciar sesión:** Se puede seleccionar este cuadro para que se realice automáticamente la conexión al iniciar sesión en el equipo donde reside físicamente este recurso.





4.1.5.11 Desconexión De Recursos Conectados

Para deshacerse de una conexión a una unidad o carpeta se la puede resaltar y pulsar el botón derecho del ratón. Hay que escoger Desconectar en el menú contextual

4.1.5.12 Permisos Para Carpetas Y Archivos

En un volumen NTFS se pueden establecer permisos a nivel de archivo. Esto significa que cualquier archivo puede otorgar a los usuarios diferentes tipos de acceso.

Se deben asignar permisos a grupos, no a usuarios individualmente. No hay que establecer permisos archivo a archivo a menos que sea inevitable.

4.1.5.13 Funcionamiento De Los Permisos

Si no se realiza ninguna acción en absoluto, los archivos y carpetas dentro de una carpeta compartida tendrán los mismos permisos que el recurso compartido. Se pueden asignar permisos tanto para directorios como para archivos a:

- Grupos locales de dominio, grupos globales, grupos universales y usuarios individuales.
- Grupos globales, grupos universales y usuarios individuales de dominios en los que confía este dominio.
- Identidades especiales como Todos y Usuarios autenticados.

Las reglas importantes para los permisos se pueden resumir como sigue:

- De forma predeterminada, una carpeta hereda permisos de su carpeta primaria. Los archivos heredan sus permisos de la carpeta en la que residen.
- Los usuarios pueden acceder a una carpeta o archivo si se les ha concedido permiso para hacerlo o si pertenecen a un grupo que tiene permiso concedido. Los permisos son acumulativos, pero el permiso Denegar prevalece sobre el resto.
- El usuario que crea un archivo o carpeta es el propietario de ese objeto y puede establecer permisos para controlar el acceso.
- Un administrador puede tomar posesión de cualquier archivo o carpeta, pero no puede ceder la propiedad a nadie más.

4.1.5.14 Configuración De Los Permisos De Las Carpetas

Antes de compartir una carpeta en un volumen NTFS, hay que establecer todos los permisos en la carpeta. Cuando se establecen permisos de carpeta se están estableciendo también permisos en todos los archivos y subcarpetas de la carpeta.

Para asignar permisos a una carpeta, hay que pulsar con el botón derecho del ratón en la carpeta en el Explorador de Windows y escoger Propiedades. Después hay que pulsar en la pestaña Seguridad y seleccionar los Permisos.

Para eliminar un individuo o grupo de la lista, basta con resaltar el nombre y pulsar Quitar.

Para añadir a la lista de aquellos con permisos, hay que pulsar el botón Agregar. Esto abre el cuadro de dialogo Seleccionar Usuarios, Equipos y Grupos.

Hay que pulsar Aceptar cuando se haya terminado y se abrirá el cuadro Permisos de carpeta con los nuevos nombres.

4.1.5.15 Asignación De Permisos A Los Archivos

Los permisos para archivos individuales se asignan de la misma forma que para las carpetas. Sin embargo, existen algunas consideraciones especiales:

- Hay que recordar el conceder permisos a grupos en lugar de a individuos.
- Hay que crear grupos y asignarles permisos de archivos en lugar de asignar permisos directamente a grupos locales.

4.1.5.16 Configuración De Permisos Especiales

En algunas circunstancias, puede ser necesario establecer, cambiar o eliminar permisos especiales bien en un archivo o bien en una carpeta. (Los permisos especiales de una carpeta sólo afectan a la carpeta.) Para acceder a los permisos especiales, hay que seguir estos pasos:

1. En el **Explorador**, hay que pulsar con el **botón derecho** del ratón en el **archivo** o carpeta y escoger **Propiedades** en el menú contextual.



2. Pulsar en la pestaña Seguridad y pulsar después el botón Avanzada.
 - **Para añadir un usuario o grupo**, hay que pulsar el botón Agregar. Hay que pulsar dos veces con el ratón en el nombre del usuario o grupo para abrir el cuadro de diálogo Entrada de permiso.
 - **Para ver o modificar los permisos especiales existentes**, hay que resaltar el nombre del usuario o grupo y pulsar el botón Ver o modificar.
 - **Para eliminar los permisos especiales**, hay que resaltar el nombre del usuario o grupo y pulsar Quitar. Si el botón Quitar está atenuado, hay que desactivar la casilla de verificación Hacer posible que los permisos heredables de un objeto primario se propaguen a este objeto y saltar al paso 6.
 - En el cuadro de diálogo **Entrada de permiso**, hay que seleccionar dónde se desean aplicar los permisos en el cuadro **Aplicar en**. Aplicar en sólo está disponible para, carpetas.
3. En Permisos hay que pulsar **Permitir o Denegar** para cada permiso.
4. Para evitar que las subcarpetas y archivos hereden estos permisos hay que seleccionar **Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor**.



4.2 Compartir Recursos Desde Linux/Unix

4.2.1 SMB (Samba)

Es la abreviatura del protocolo bloque de mensajes del servidor, y es el protocolo estándar que utiliza la familia windows NT para compartir servicios de archivos e impresión. SMB opera de la forma petición-respuesta, donde los clientes envían peticiones, contenidas en bloques de mensajes de servidor (smb), al servidor. Este, recibe lossmb, los interpreta y envía de regreso la respuesta al cliente. Cuando un ordenador comparte un recurso a través de la red por medio de smb, se convierte en un servidor en este escenario. Cuando un ordenador accede a un recurso compartido, se convierte en un cliente.

La comunicación mas habitual en entornos mixtos Linux/Unix y NT/2000/Xp se realiza a través de NetBIOS a través de TCP/IP.

Una vez que el cliente se conecta al servidor y se autentica, el cliente puede proceder a enviar ordenes al servidor para abrir , leer o escribir, cerrar, eliminar archivos, y ejecutar otras ordenes de directorio.

El protocolo SMB proporciona dos niveles de seguridad en sus modelos de seguridad. El primer modelo es nivel de seguridad del recurso compartido, bajo el cual , a los recursos compartidos se les asigna una contraseña, la cual garantiza el acceso a ellos. Con el nivel de seguridad de usuario las protecciones de los accesos se aplican a archivos individuales y los derechos de acceso se determinan en base al usuario. Al usuario le tiene que autenticar el servidor del recurso compartido y asignarle un ID numérico de usuario. Este ID se compara después con las protecciones de acceso asignadas a cada archivo.

Nos basaremos en la distribución Debian para explicar la configuración de un servidor Samba, debido al carácter mas abierto de dicha distribución y a su ajustada política GNU.

Primero debemos instalar los paquetes *Samba* y *Samba-common*. En caso de tener conexión a Internet y tener bien configurado nuestro fichero sources.list, el comando a utilizar seria :

- **apt-get install Samba Samba-common**

Tras instalarlo, podemos pasar a editar el fichero de configuración, que dependiendo del sistema en el que nos encontremos, podremos localizar en distintos directorios. En este caso lo haremos mediante el editor *vim* (vi mejorado) en la ruta:

- `vim /etc/Samba/smb.conf`

El fichero es grande, pero se encuentra dividido en secciones, lo que facilita mucho su edición. En el caso que nos ocupa, las secciones mas importantes serán *[global]*, que establece las variables de configuración de todos los recursos, *[homes]*, que permite acceder a un usuario de Linux a su directorio \$HOME desde una maquina Windows, *[printers]*, que especifica la configuración de las impresoras compartidas. También podremos crear nosotros una sección nueva, indicando el recurso que queramos compartir, y los parámetros que la definan.

4.2.1.1 Sección *[global]*

Aquí especificaremos los valores generales, tales como el nombre del servidor, el nombre del grupo de trabajo (en el ejemplo, *mired*), el nivel de seguridad (habitualmente *user*), o la encriptación de las contraseñas.

Podemos observar como , en la línea *guest account* se deniega el acceso a invitados en el sistema al indicar *nobody* (habitualmente un usuario valido sin privilegios que no puede iniciar sesión). También se desactiva el acceso al *root* por cuestiones de seguridad.

```
[global]
# Be something sensible when Samba crashes: mail the admin a backtrace
panic action = /usr/share/samba/panic-action %d
printing = bsd
printcap name = /etc/printcap
load printers = yes
guest account = nobody
invalid users = root

# "security = user" is always a good idea. This will require a Unix account
# in this server for every user accessing the server.
security = user

# Change this for the workgroup your Samba server will part of
workgroup = mired

server string = %h server (Samba %v)

syslog only = no
syslog = 0;

# These socket options really speed up Samba under Linux, according to my
# own tests.
socket options = IPTOS_LOWDELAY TCP_NODELAY SO_SNDBUF=4096 SO_RCVBUF=4096
encrypt passwords = true
passdb backend = smbpasswd guest

wins support = no
```


4.2.1.2 Sección [homes]

En ella encontramos los parámetros de acceso a los directorios personales de los usuarios remotos de la máquina Linux. Especificamos desde el acceso o no a los citados recursos, como los permisos por defecto que se establecerán. El campo *browseable* indicará si se enseñará los directorios raíz en la lista del explorador de red. Tanto *create mask* como *directory mask* especifican los permisos por defecto que se aplicarán a ficheros y directorios

```
[homes]
  comment = Home Directories
  browseable = yes

# By default, the home directories are exported read only. Change next
# parameter to "no" if you want to be able to write to them.
  read only = no

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group-rw permissions, set next parameter to 0775.
  create mask = 0744

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group-rw permissions, set next parameter to 0775.
  directory mask = 0744
```

4.2.1.3 Sección [printers]

Especificaremos los parámetros necesarios de configuración necesarios. *Printable* le indica al sistema que es un recurso de impresión, y *public* activa o desactiva la cuenta de *invitado*. *Writable* indica un valor no, ya que es un recurso de impresión, no uno de sistemas de ficheros.



```
[printers]
comment = All Printers
browseable = no
path = /var/spool/samba
printable = yes
public = yes
writable = no
```

Podremos crear, asimismo una sección personalizada, con los parámetros del recurso que queramos compartir (ruta del recurso, permisos a establecer, etc..). En ella podremos definir múltiples parámetros. La línea *path* indica el directorio a compartir, y *public* indica la desactivación del acceso a invitados.

```
[compartir]
comment = Directorios compartidos
browseable = yes
path = /mis_ficheros
public = no
writable = yes
create mode = 0700
```

4.2.1.4 Seguridad En SAMBA

Existen tres tipos de seguridad en Samba en la actualidad bajo sistemas Unix/Linux, definiéndose en el fichero *smb.conf*:

Seguridad del recurso compartido

Mediante la opción *share*, se restringe el acceso basándose en los permisos del recurso compartido. El nivel más bajo de seguridad.



Seguridad de usuario

La opción `user` indica al servidor Samba que debe utilizar el nombre de usuario como validación de acceso al recurso compartido. La validación se realiza en el archivo local de contraseñas. Este sistema obliga a mantener un amplio archivo local de contraseñas, por lo que algunos administradores de sistemas no están muy a favor de usarlo.

Seguridad de servidor

Samba permite redireccionar todas las autenticaciones a un servidor SMB distinto (incluso un windows NT). La opción a usar sería:

```
security=server
```

```
password server=NTSRV (nombre del servidor de autenticación)
```

Para la creación de un usuario Samba podemos utilizar el comando `smbpasswd`. Mediante la utilización del parámetro `-a`, podemos incluir a un usuario en la lista de usuarios de Samba, así como asignarle una contraseña

```
smbpasswd -a usuario1
```

Hasta aquí hemos abordado la configuración del servidor Samba desde una consola. Existe un modo gráfico de configuración adicional: la aplicación SWAT. Mediante una interfaz web es posible realizar toda la configuración del servidor. Para activar `swat` únicamente hay que añadir (o descomentar) esta línea en el fichero `/etc/inetd.conf`

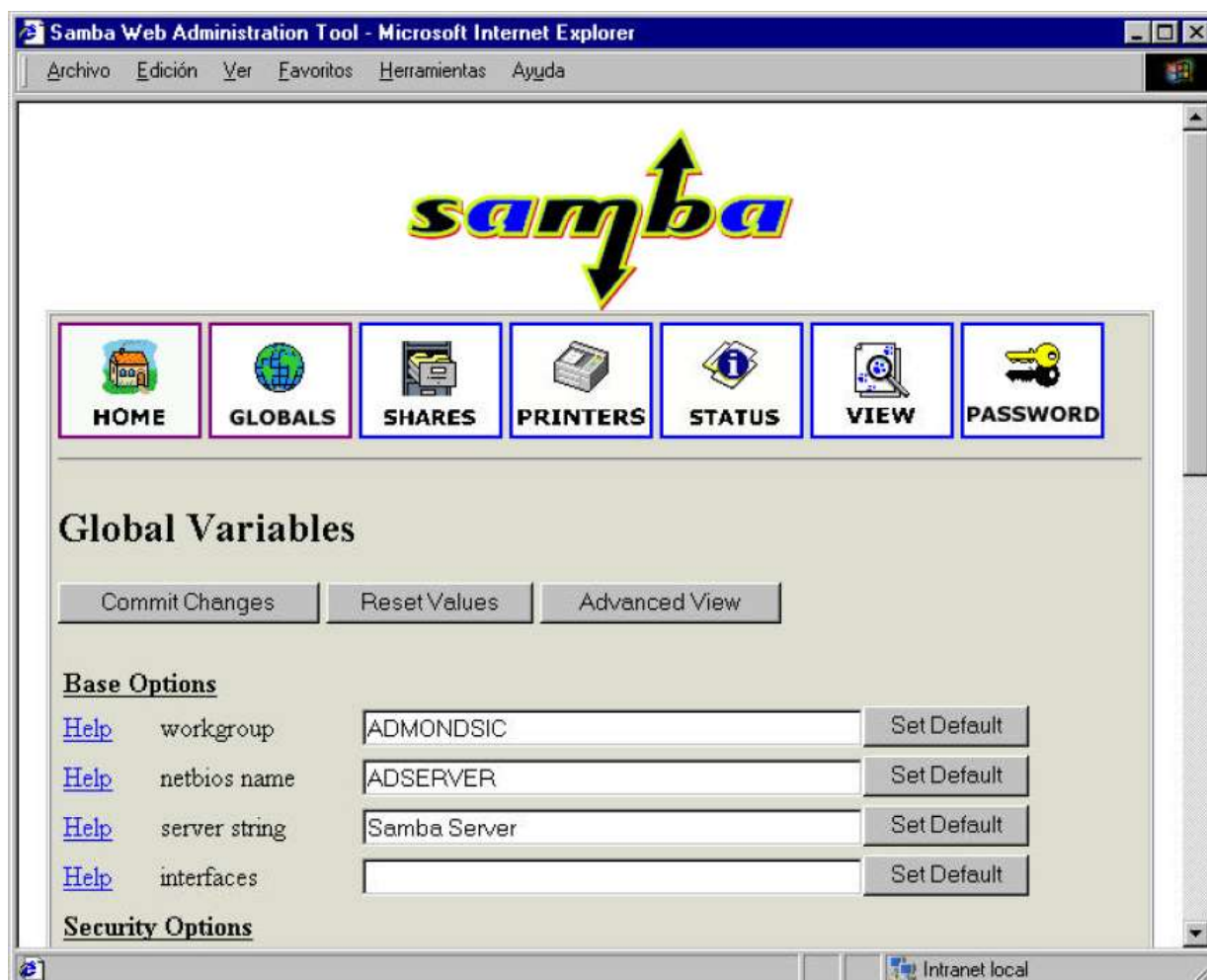
```
swat stream tcp nowait.400 root /usr/sbin/tcpd /usr/sbin/swat
```

Posteriormente hemos de incluir en `/etc/services` la siguiente línea:

```
swat 901/tcp
```

A continuación, y reiniciando el servicio `inetd` (`/etc/init.d/inetd restart`) tendremos `swat` listo para ser accedido a través de interfaz web, mediante `http://dirección_ip:901`.





Tras la instalación y configuración, podremos lanzar manualmente los daemon necesarios (mediante el comando `/etc/init.d/Samba start`), o bien reiniciar la maquina para que se inicien con el sistema.

En cualquier caso , los dos daemon necesarios serán **smbd** (encargado de proporcionar los servicios Samba) y **nmbd** (proporciona soporte para NetBIOS). Mediante el comando `ps -e` podremos verificar que se encuentren ejecutándose en memoria.

4.2.2 NFS (Network File System)

Nació en 1984 y se convirtió en un estándar para los servicios de archivos en los entornos de redes multiconvencionales: NFS oculta os detalles sobre donde se almacenan físicamente los archivos, pudiendo estar en cualquier maquina, y que parezcan como parte del sistema de archivos local. Esto permite una utilización transparente para el usuario, y una centralización de los datos para el administrador.

Nfs utiliza principalmente dos protocolos : XDR (representación externa de datos)y RPC (llamadas a procedimientos remotos. RPC proporciona las bases para el intercambio de mensajes entre clientes y servidores, y XDR la traducción de datos entre distintos tipos de ordenadores y sistemas operativos.

Para su funcionamiento es necesario configurar el kernel del servidor (habitualmente implementada por defecto en todas las distribuciones modernas), y la instalación de los daemons necesarios (en este caso serán necesariosnfsd y rpc.mountd)

La instalación , siempre basándonos en Debian, seria :

```
apt-get install nfs-common nfs-kernel-server
```

Una vez instalado, podremos acudir al fichero encargado de definir los recursos a compartir, y los permisos de acceso. Este fichero es

/etc/exports.

El primer valor a indicar sera el directorio que queramos que sea accesible desde la red, seguido por las máquinas que tendrán acceso a el, y los permisos asociados a ellas.

```
/home                                maquina1(rw) maquina2(rw) maquina3(ro)
```

```
/mis_ficheros                        172.26.0.101(rw)
```

Es posible el uso de comodines, así como valores que autoricen a una red completa

```
/mis_ficheros                        172.26.0.255/255.255.255.0(rw)
```



Las opciones indicadas entre paréntesis mas habituales pueden ser :

insecure	permite acceso no autenticado.
kerberos	requiere autenticación Kerberos.
root_squash	deniega el acceso a superusuario por seguridad.
ro	monta el sistema de ficheros en solo lectura (por defecto).
rw	monta el sistema de ficheros en modo lectura/escritura.

Existen otras opciones menos utilizadas, tales como :unix-rpc, secure-rpc, link_relative, link_absolute,

Una vez modificado el fichero `/etc/exports` se pueden reiniciar los daemon encargados, o bien mediante el comando *exportfs*, actualizar la tabla de exportaciones para incluir las modificaciones realizadas.

Es importante indicar el bajo nivel de seguridad del sistema de ficheros NFS, debido en parte a su creación en los primeros tiempos de las redes UNIX, así como los problemas de permisos que se crean , ya que se asignan permisos en función del **UID** del usuario en la maquina servidor.

Actualmente se esta trabajando en una implementación NFS mas adaptada a las nuevas condiciones de las redes modernas.

