UNIDAD 5

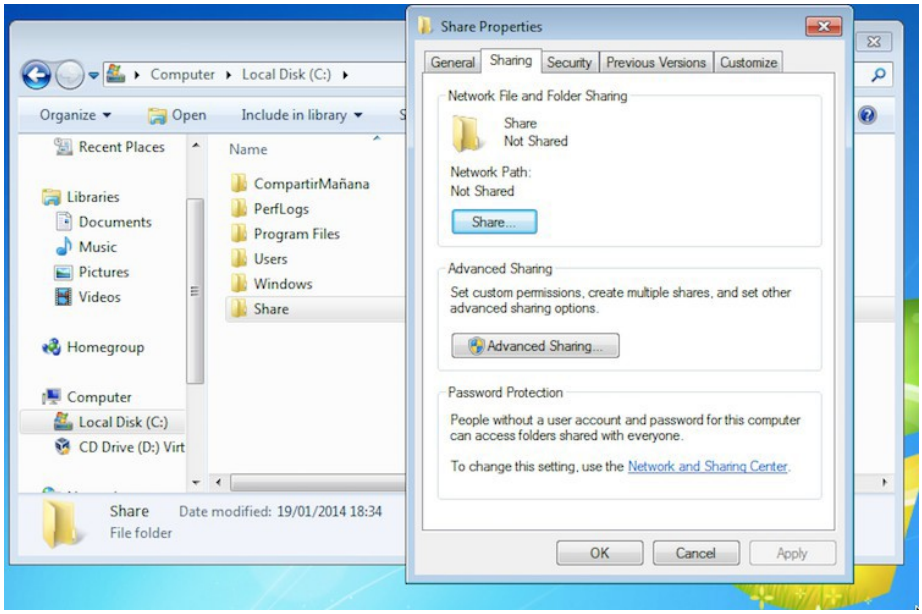
Compartir recursos en red (Windows y Linux)

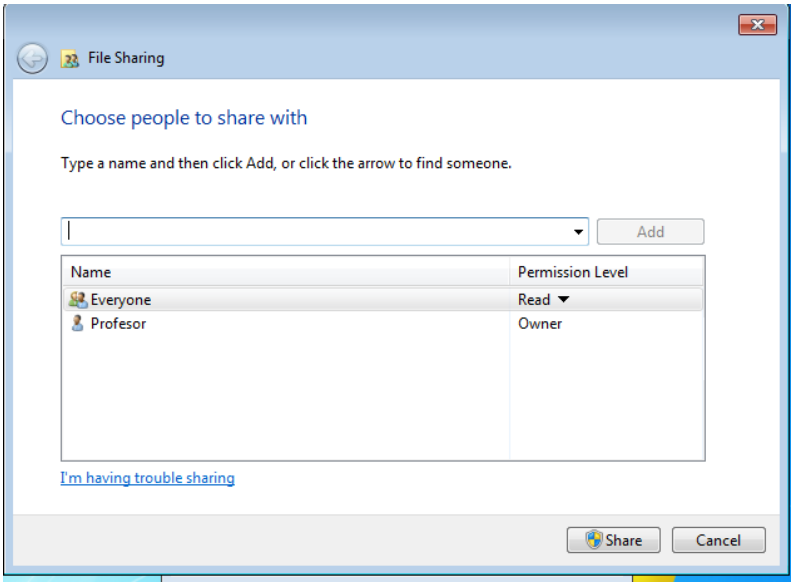
Sistemas Informáticos
1º de DAW Semipresencial
IES San Vicente 20/21

Index

Compartir carpetas en Windows

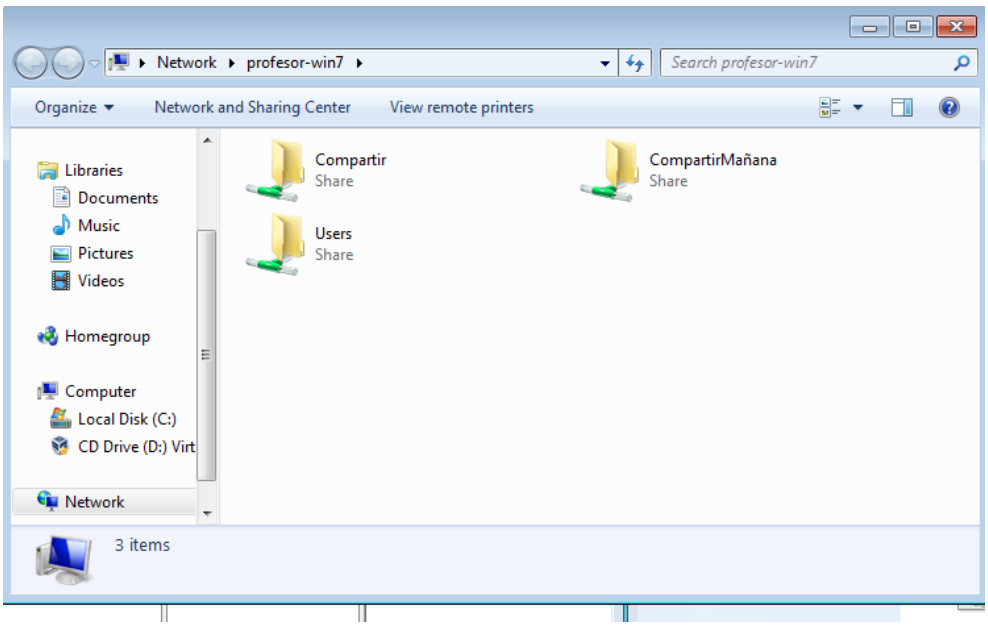
Si queremos compartir una carpeta, debemos pulsar con el botón derecho del ratón sobre la carpeta. Entonces seleccionaremos la pestaña de compartir. En esta tendremos disponibles las opciones de compartir. En las opciones avanzadas tendremos disponibles los permisos sobre usuarios y grupos.



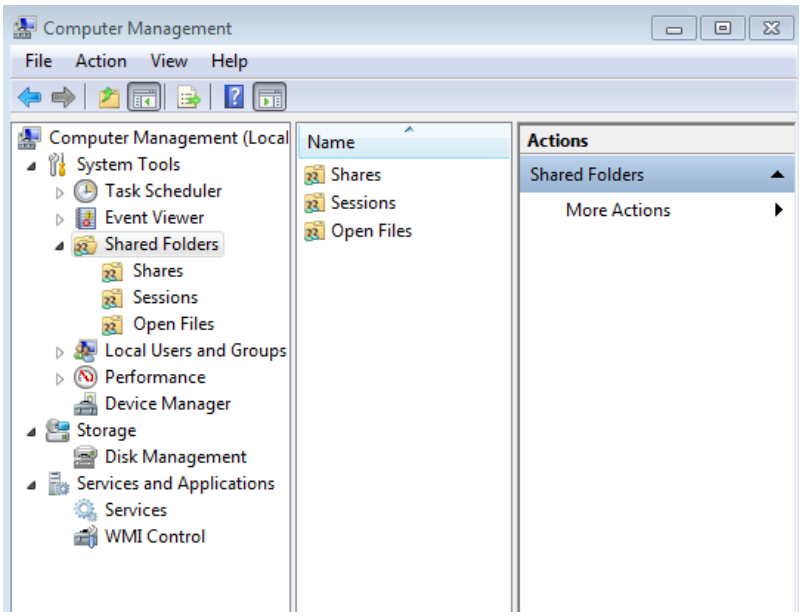


Podemos acceder a la carpeta compartida a través de la ruta UNC (Universal Naming Convention) \\Nombre_NetBios o \\Server_IP

Dependido de la configuración del servidor se podrá mostrar una ventana de autentificación. Una vez que tengamos acceso veremos una pantalla como la de la imagen siguiente y en ellas podremos explorar la carpeta compartida.



Podemos acceder a la información sobre las carpetas compartidas a través de diferentes herramientas. Administración de equipos (Panel de control→Herramientas administrativas→Administración de equipos).



Directorio Activo (Windows Server)

Servicios de directorio

Los Servicios de Directorio de Active Directory almacenan información sobre la organización, sitios, ordenadores, usuarios, objetos compartidos y cualquier otra cosa que pueda formar parte de la infraestructura de red. Lo elementos de Directorio Activo pueden ser diferentes unos de otros (usuarios, grupos, políticas de acceso, permisos, asignación de recursos, etc.), por lo que la información almacenada variará según la naturaleza del objeto. Toda esta información se almacena en una base de datos jerárquica.

Directorio

Un Directorio es un repositorio único para la información relativa a los usuarios y recursos de una organización. Active Directory es un tipo de directorio y contiene información sobre las propiedades y la ubicación de los diferentes tipos de recursos dentro de la red. Usándolo, tanto los usuarios como los administradores pueden encontrarlos con facilidad.

Una de las ventajas que ofrece Active Directory es que puede utilizar LDAP (Lightweight Directory Access Protocol, en español, Protocolo Ligero de Acceso a Directorios), un protocolo de acceso estándar que permitirá la consulta de información contenida en el directorio. Sin embargo, también puede utilizar ADSI (Active Directory Services Interface, en español, Interfaces de Servicio de Active Directory), un conjunto de herramientas ofrecidas por Microsoft, que tienen una interfaz orientada a objetos y que permiten el acceso a características de Active Directory Domain Services que no están soportadas por LDAP.

Dominio

Un Dominio es una colección de objetos dentro del directorio que forman un subconjunto administrativo. Pueden existir diferentes dominios dentro de un bosque, cada uno de ellos con su propia colección de objetos y unidades organizativas.

Para poner nombre a los dominios se utiliza el protocolo DNS. Por este motivo, Active Directory necesita al menos un servidor DNS instalado en la red.

Objeto

Cualquiera de los componentes que forman parte del dominio, como una impresora o una carpeta compartida, pero también un usuario, un grupo, etc.

Cada objeto dispondrá de una serie de características específicas (según la clase a la que pertenezca) y un nombre que permitirá identificarlo de forma precisa. Las características específicas de cada tipo de objeto quedarán definidas en el Esquema de la base de datos.

En general, los objetos se organizan en tres categorías:

- **Usuarios**: identificados a través de un nombre (y, casi siempre, una contraseña), que pueden organizarse en grupos, para simplificar la administración. Desde un punto de vista informático, un usuario es un conjunto de permisos y de privilegios sobre determinados recursos. En este sentido, un usuario no tiene que ser, necesariamente, una persona.

- **Recursos**: que son los diferentes elementos a los que pueden acceder, o no, los usuarios según sus privilegios. Por ejemplo, carpetas compartidas, impresoras, etc.

- **Servicios**: que son las diferentes funciones a las que los usuarios pueden tener acceso. Por ejemplo, el correo electrónico.

Unidad Organizativa

Una Unidad Organizativa es un contenedor de objetos que permite organizarlos en subconjuntos, dentro del dominio, siguiendo una jerarquía. De este modo, podremos establecer una estructura lógica que represente de forma adecuada nuestra organización y simplifique la administración.

Otra gran ventaja de las unidades organizativas es que simplifican la delegación de autoridad (completa o parcial) sobre los objetos que contienen, a otros usuarios o grupos. Esta es otra forma de facilitar la administración en redes de grandes dimensiones.

Controlador de dominio

Cuando instalamos Active Directory en un ordenador con Windows Server, convertimos a ese ordenador en un Controlador de dominio. Un Controlador de dominio (domain controller) contiene la base de datos de objetos del directorio para un determinado dominio, incluida la información relativa a la seguridad. Además, será responsable de la autenticación de objetos dentro de su ámbito de control.

En un dominio dado, puede haber varios controladores de dominio asociados, de modo que cada uno de ellos represente un rol diferente dentro del directorio. Sin embargo, a todos los efectos, todos los controladores de dominio, dentro del mismo dominio, tendrán la misma importancia.

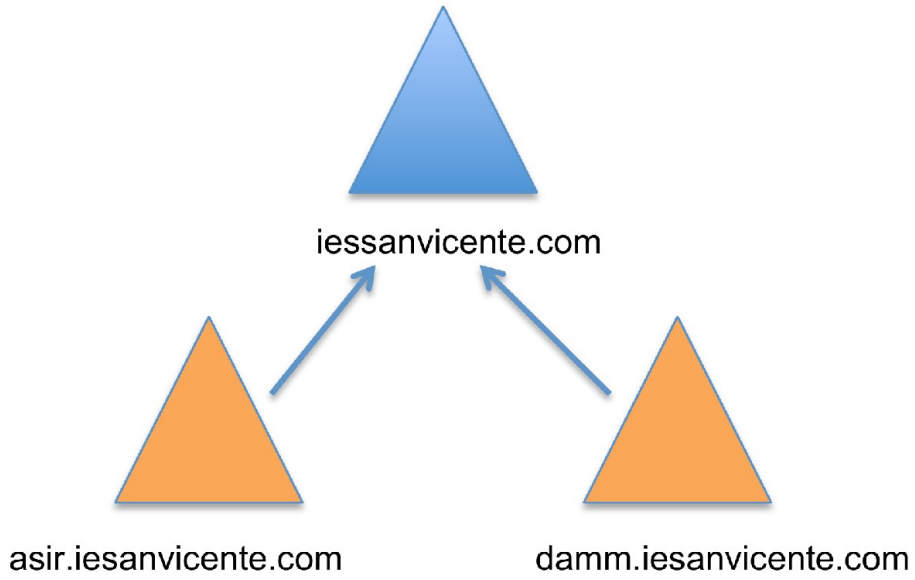
Árboles

Un Árbol es simplemente una colección de dominios que dependen de una raíz común y se encuentra organizados como una determinada jerarquía. Dicha jerarquía también quedará representada por un espacio de nombres DNS común.

De esta forma, sabremos que los dominios **iessanvicente.com** y **damm.iessanvicente.com** forman parte del mismo árbol, mientras que**iessanvicente.com** y **iessanvicente.es** no.

El objetivo de crear este tipo de estructura es fragmentar los datos del Directorio Activo, replicando sólo las partes necesarias y ahorrando ancho de banda en la red.

Si un determinado usuario es creado dentro de un dominio, éste será reconocido automáticamente en todos los dominios que dependan jerárquicamente del dominio al que pertenece.



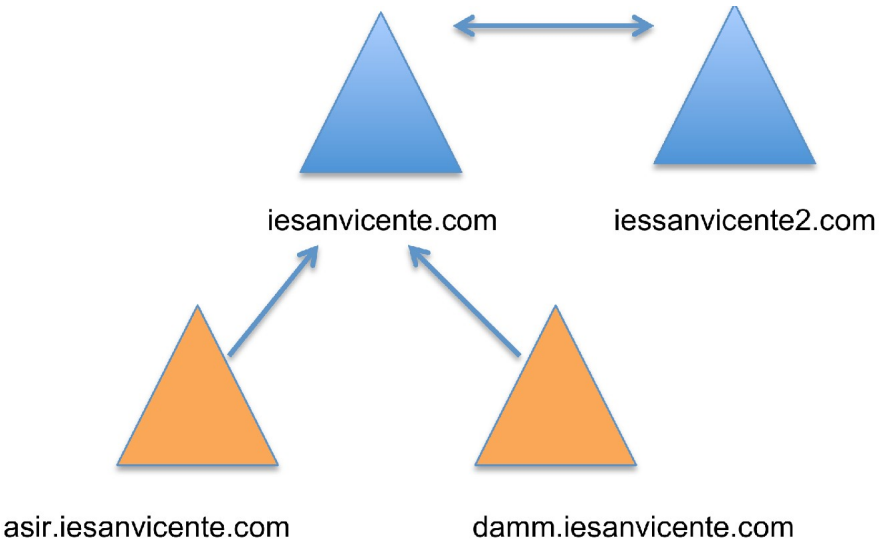
Bosque

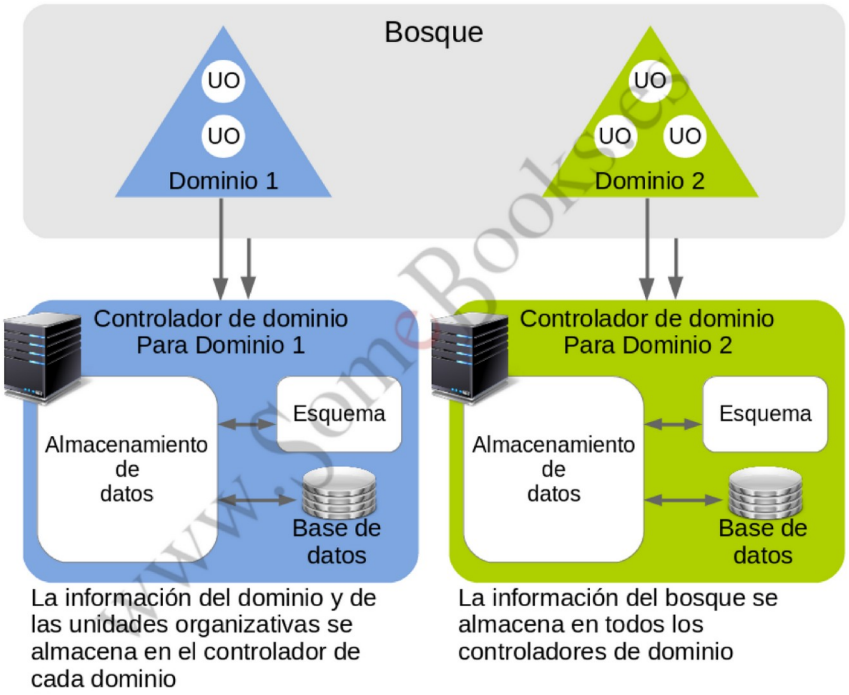
El Bosque es el mayor contenedor lógico dentro de Active Directory, abarcando a todos los dominios dentro de su ámbito. Los dominios están interconectados por Relaciones de confianza transitivas que se construyen automáticamente (consultar más adelante el concepto de Relación de confianza). De esta forma, todos los dominios de un bosque confían automáticamente unos en otros y los diferentes árboles podrán compartir sus recursos.

Como ya hemos dicho, los dominios pueden estar organizados jerárquicamente en un árbol que comparte un espacio de nombres DNS común. A su vez, diferentes árboles pueden estar integrados en un bosque. Al tratarse de árboles diferentes, no compartirán el mismo espacio de nombres.

De forma predeterminada, un bosque contiene al menos un dominio, que será el dominio raíz del bosque. En otras palabras: cuando instalamos el primer dominio en un ordenador de nuestra red que previamente dispone de Windows Server, además del propio dominio, estamos creando la raíz de un nuevo árbol y también la raíz de un nuevo bosque.

El dominio raíz del bosque contiene el Esquema del bosque, que se compartirá con el resto de dominios que formen parte de dicho bosque.





Esquema

En Active Directory Domain Services se utiliza la palabra Esquema para referirse a la estructura de la base de datos. En este sentido, utilizaremos la palabra atributo para referirnos a cada uno de los tipos de información almacenada.

También suele emplearse una terminología orientada a objetos, donde la palabra Clase se referirá a un determinado tipo de objetos (con unas propiedades determinadas), mientras que un objeto determinado recibe el nombre de instancia. Por ejemplo, podríamos pensar que la clase usuario es una plantilla que definirá a cada uno de los usuarios (que serán instancias de la clase usuario).

Sitio

Un Sitio es un grupo de ordenadores que se encuentran relacionados, de una forma lógica, o con una localización geográfica particular. En realidad, pueden encontrarse físicamente en ese lugar o aunque no lo estén, como mínimo, estar conectados mediante un enlace permanente con el ancho de banda adecuado.

En otras palabras, un controlador de dominio puede estar en la misma zona geográfica de los clientes a los que ofrece sus servicios o puede encontrarse en el otro extremo del planeta (siempre que estén unidos por una conexión adecuada). Pero en cualquier caso, todos juntos formarán el mismo sitio.

GPO (Group Policy Object)

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:

- Establecer el título del explorador de Windows
- Ocultar el panel de control
- Deshabilitar el uso de REGEDIT.EXE y REGEDT32.EXE
- Establecer qué paquetes MSI se pueden instalar en un equipo

Podemos definir dos categorías de tipos troncales de directivas:

1. Según su función
2. Según su el objeto que configuran

Directivas según su función:

- **Directivas de seguridad**. Como por ejemplo: ¿Cuántos carácteres tiene una contraseña? ¿Cada cuanto tiempo debe ser cambiada ésta?, etc. Pueden ser aplicadas:
    - A nivel de dominio: Son aplicadas en todas las máquinas del dominio.
    - A nivel particular de controlador de dominio: Se aplican tan sólo en los controladores de dominio, pero sin suplantar a las generales del dominio (en caso de entrar en contradicción una y otra, se aplica la del dominio, no la de los controladores de dominio).
- **Directivas de entorno (GPO → Group Policy Object)**. Como por ejemplo: 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 nivel de equipo local
    - A nivel de sitio
    - A nivel de dominio
    - A nivel de Unidad Organizativa (OU -> Organizational Unit).

Directivas según el objeto que configuran:

- **Configuración del equipo**: que se divide en:
  - Configuración de software
  - Configuración de Windows
  - Plantillas administrativas
- **Configuración del usuario**, que se divide en:
  - Configuración de software
  - Configuración de Windows
  - Plantillas administrativas

Aunque las configuraciones de equipo y usuario se dividan en las mismas partes, dentro de éstas son diferentes las políticas que se encuentran.

¿Qué objetos son los contenedores de las GPO's?

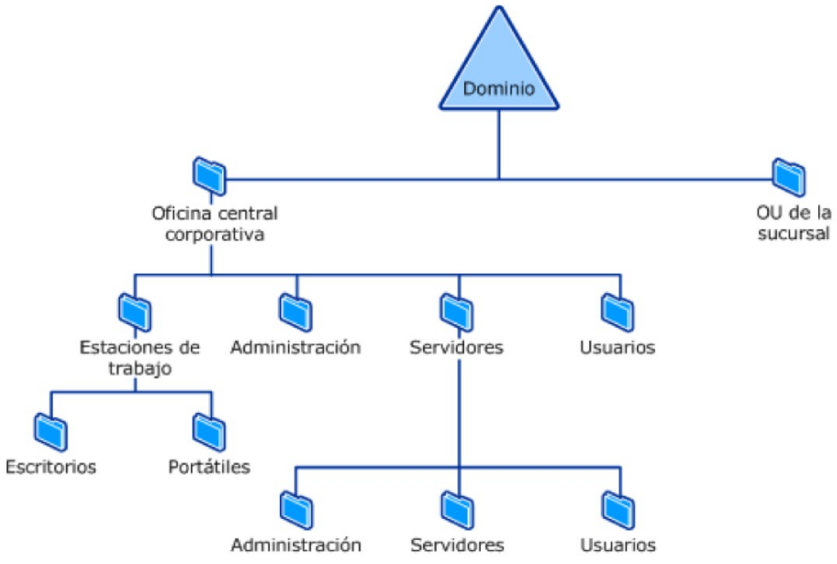
Las GPO's pueden estar contenidas en cuatro tipos de objetos:

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(standalone) o clientes en red igual a igual (peer to peer).

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 a los equipos y/o usuarios que pertenezcan a la propia unidad organizativa (OU).



Compartir carpetas con SAMBA (Linux)

SAMBA es una implementación para sistemas operativos Linux, UNIX y MAC de una serie de protocolos utilizados en Windows para: Compartir archivos, servicio de nombres NETBIOS para identificar máquinas en una red local, servicio de impresión, autenticación en Active Directory, servicios de dominio, etc...

La configuración de SAMBA se edita a mano desde el archivo **/etc/samba/smb.conf**. También desde otras herramientas gráficas como Webmin, SWAT, o las que incorporan escritorios como Gnome o KDE.

La configuración más básica de SAMBA implica unirse a un grupo de trabajo (sin servidor de dominio) para compartir archivos e impresoras en red. Puede configurarse para entrar en un dominio, o para ser controlador de dominio. Todo esto interactuando sin problemas con máquinas Windows.

Para usar SAMBA debemos instalar los paquetes **samba, samba-common, smbclient, cifs-utils**.

Los bloques de configuración (1 por cada recurso compartido), están delimitados con el nombre entre corchetes en el archivo de configuración, siendo [global] el que contiene la configuración general de SAMBA.

Ejemplo de configuración de carpeta compartida:

```
[share]
  writeable = yes
  path = /home/share/samba-share/
  admin users = sambauser
  valid users = sambauser usuario1
  read list = usuario1
  public = yes
  available = yes
```

Configuración global

Dentro del bloque [global], que afecta a todos los recursos compartidos de forma global, podemos encontrar (entre otros) los siguientes parámetros de configuración:

- **workgroup** → Nombre del grupo de trabajo al que pertenecerá la máquina.
- **netbios name** → Nombre que tendrá la máquina en una red Windows (coincidirá con el nombre que le hayamos dado al equipo en la instalación por defecto).
- **server string** → Nombre que aparecerá en la ubicación de las impresoras compartidas. %h se sustituye por el nombre de la máquina.
- **Security**: Tipo de seguridad a nivel de autenticación de usuarios. Los valores pueden ser:

    - **user** → Recomendada por defecto, los usuarios deberán usar un nombre de usuario y contraseña del equipo.

    - **share** → No requiere usuario y contraseña. Inseguro.

    - **domain** → Sólo cuando se forme parte de un dominio. El usuario debe ser válido en nuestra máquina y en el controlador de dominio.

    - **server** → Valida el usuario con otro servidor, si esto falla, lo valida en la propia máquina.

- **guest account** → usuario del sistema que se utilizará por defecto cuando se acceda de forma anónima a un rescurso compartido. En muchos sistemas existe un usuario llamado nobody para estas funciones, pero se puede usar cualquiera (también existe un grupo llamado nogroup).

- **map to guest** → Indica cuando un usuario se conectará como anónimo (guest account) teniendo en cuenta que vamos a pedir usuario y contraseña. No tiene sentido si usamos security = share por ejemplo:

    - Never → Por defecto. No se permiten usuarios anónimos.

    - Bad User → Cuando el nombre de usuario introducido no exista.

    - Bad Password → Cuando el password sea incorrecto. Este método no es muy recomendable ya que el sistema no avisará al usuario de que ha introducido mal la contraseña y entrará como invitado.

- **unix password sync** → valores yes o no. Indica si cuando se cambia la contraseña del usuario SAMBA (se puede usar una contraseña diferente para acceder mediante samba a los recursos compartidos y para entrar al equipo de forma normal), se cambiará también su contraseña (se pondrá la misma) para el login en el equipo.

- **invalid users** → Lista de usuarios (separados por espacio). Impide el login de los usuarios listados aquí en SAMBA. Si queremos especificar un grupo, en lugar de un usuario, pondremos una '@' delante del nombre del grupo.

- **valid users** → Mismo formato que arriba. Si está vacía, cualquiera puede entrar (excepto si está en la lista de arriba). Si se pone algún usuario la cosa cambia y SÓLO esos usuarios pueden entrar. Si algún usuario está afectado por las dos listas se le niega el acceso.

- **admin users** → Usuarios que tendrán todos los privilegios (como si fueran root) en los recursos compartidos (cuidado con esta opción).

- **read list** → Lista de usuarios que tendrán permisos de sólo lectura en los recursos compartidos independientemente del atributo read only que haya en el recurso compartido.

- **write list** → Usuarios que tendrán permiso de lectura y escritura en los

recursos compartidos. Esta lista tiene preferencia sobre la de solo lectura, por lo que quien esté afectado por ambas, seguirá pudiendo escribir.

- **hosts allow** → lista de máquinas que podrán conectarse (vacía significa que todas). Puede usarse el nombre de la máquina, su ip, o una ip de red (ip/máscara). Se puede especificar despues qué máquinas (de esas redes) se excluyen poniendo la palaba EXCEPT seguida de las máquinas.
    - hosts allow = 192.168.0.0/24 EXCEPT 192.168.0.27
- **hosts deny** → máquinas que tienen prohibido el acceso. Si se va a usar una política de prohibir a todos el acceso excepto a los que estén en hosts allow, se debe usar la palabra ALL o la dirección 0.0.0.0/0.
    - Tiene prioridad la lista hosts allow sobre esta.
    - Si queremos usar política permisiva (permitir a todos excepto los que estén en hosts deny, se debe dejar la lista de hosts allow vacía)

Compartir carpetas

Para cada recurso compartido se debe crear una sección, con nombre del recurso compartido entre corchetes (el nombre puede ser diferente al de la carpeta que se comparte y será el que aparecerá cuando se acceda remotamente). Después del nombre, y hasta el final del archivo o hasta que comience el siguiente recurso compartido, se pondrán las opciones de compartición de ese recurso.

Las listas **invalid users, valid users, admin users, read list, write list, hosts allow y hosts deny** funcionan exactamente igual que en la configuración global, pero esta vez sólo afectan al recurso compartido (y tendrán preferencia sobre las globales).

- **comment** → Descripción del recurso compartido.
- **path** → ruta (absoluta) al directorio/carpeta compartido.
- **read only** → valores yes o no. Si activamos esta opción (yes) se compartirá en modo sólo lectura por defecto (excepto para usuarios que estén en write list).
- **writable** → Equivalente a read only pero contrario en cuanto al significado (yes indica que se puede leer y escribir y no, solo lectura). No tiene sentido usar ambas a la vez.
- **guest ok** → (yes, no).Permite que usuarios anónimos puedan acceder (con la cuenta definida en guest account). Si la seguridad es diferente de security = share (por defecto el valor es user), necesitamos tener habilitada la opción map to guest en globales para que alguien pueda loguearse de forma anónima.
- **browseable** → (yes,no). Indica si la carpeta aparecerá cuando se listen los recursos compartidos de una máquina o estará oculta (se deberá conocer la url para acceder).

- **available** → (yes,no). Deberá estar activada para permitir acceder a este recurso independiente de la configuración anterior. Por defecto lo está.

Añadir usuarios a SAMBA

Podemos añadir un usuario existente en el sistema a SAMBA asignándole una contraseña con el comando:

smbpasswd -a usuario

La contraseña no tiene por qué ser la misma que la asignada para la autenticación en el sistema (/etc/shadow), aunque si se activa la opción unix password sync, sí que se mantendrá la misma contraseña para SAMBA y login de usuario.