



BULMA

Bisoños Usuarios de Linux de Mallorca y Alrededores | Bergantells Usuaris de Linux de Mallorca i Afegitons



Configurar un servidor de Samba - Módulo 4.1.3

Por Daniel Rodriguez, [DaniRC](http://bulma.net/~danirc/) (<http://bulma.net/~danirc/>)

Creado el 11/06/2002 12:16 y modificado por última vez el 11/06/2002 12:16

Vamos a configurar Samba paso a paso, conociendo de manera didáctica la mayor parte de la funcionalidad de este servidor.

Al final del artículo, deberíamos ser capaces de [pegarle una patada a nuestros NT's](#) ... o al menos saber convivir con ellos de manera elegante.

De nuevo agradecer a MandrakeCampus la licencia LGPL sin la cual estas traducciones no serian posibles.

Nivel : Avanzado

Documento original: www.mandrakecampus.com

Traducción al castellano : Daniel Rodríguez

Documento realizado con [OpenOffice 1.0](#)

[Licencia LGPL](#)

Indice

1. La comparticion de recursos
2. ¿ Qué es Samba ?
3. Presentación de los servidores
4. SWAT la herramienta de configuración gráfica.
5. Teoria de funcionamiento de CIFS
6. Configuracion de parámetros globales
7. Comparticion de Impresoras, directorios y modalidades de compartición (guest/invitado) y otras
8. Integración de Samba en un dominio NT
9. Configuracion de Samba como controlador de dominio

10. Herramientas del cliente. Smbmount, smbtar, ...

11. Para profundizar ...

La compartición de recursos

Inconvenientes del servicio de FTP

El servicio de FTP permite intercambiar ficheros en red. Pero presenta serios problemas de integración: Su uso no es transparente, es decir, cambia según tratemos con estaciones de trabajo Unix o Windows.

NFS, una solución limitada a máquinas UNIX

Entre máquinas Unix, es posible usar el protocolo NFS para compartir ficheros. Se trata de una gran solución puesto que permite conservar todas las funcionalidades del sistema de ficheros Unix. Aun así, presenta una serie de inconvenientes :

- NFS presenta problemas de seguridad.
- No existe una buena implementación libre de NFS para equipos Windows.

La solución: utilizar el protocolo CIFS

En lugar de usar una solución, costosa, en los equipos Windows, es más económico -y lleva menos trabajo- utilizar el protocolo utilizado nativamente por las máquinas Windows. Este protocolo, llamado **Common Internet FileSystem** (CIFS), tiene implementaciones sobre un gran número de plataformas.

Existe una implementación libre de este protocolo llamada Samba, que permite utilizarlo sobre servidores Unix

¿ Qué es Samba ?

Presentación de Samba

Samba es una implementación bajo Unix de los protocolos CIFS y NetBIOS (antiguamente llamado SMB, de allí el nombre de SAMBA)

Este protocolo permite compartir varios recursos diferentes:
El acceso a las impresoras conectadas físicamente a las máquinas.
El acceso a los directorios compartidos.

La paquete de SAMBA incluye utilidades para controlar el acceso de los archivos con la misma soltura que un WindowsNT. Además Samba puede colaborar con un servidor NT existente, o reemplazarlo del todo.
Veremos más adelante como configurarlo en detalle, pero es posible:

- Proteger por contraseña el acceso a un directorio compartido.
- Proteger con una contraseña personalizada para cada usuario, y dotar de permisos de acceso individualizados.

Las herramientas necesarias

Paquetes a instalar

Los paquetes de samba suelen ser 3 (almenos en la distribucion Mandrake):

1. samba-common
2. samba
3. samba-client

El primer paquete tiene los elementos que van a permitir el buen funcionamiento de los otros dos: Las herramientas de conversion de tablas de caracteres Windows, los ficheros de configuracion y la documentacion.

El segundo paquete contiene todos los programas del servidor, es decir: aplicaciones que permiten hacer accesible los recursos a los usuarios, herramientas de configuracion y la documentacion esencial de Samba.

El ultimo paquete contiene los programas clientes, que permiten acceder a los recursos compartidos

Proceso de instalacion

Los paquetes se pueden instalar facilmente con urpmi (la utilidad tipo apt de mandrake) si estas conectado a la Internet. O bien desde el CD-ROM de la distribucion. En todo caso se aconseja instalar los 3 paquetes anteriores y tal vez el paquete swat que es una aplicacion web que te permite configurar tu servidor Samba facilmente. Pero para ello te hara falta el apache y varias dependencias mas, asi que con los 3 paquetes de Samba nos bastara para empezar.

Personalmente lo que mas me gusta es lanzar

```
# urpmi samba*
```

Nota: Versiones antiguas de urpmi se quedaban bastante colgadas. La ultima version obtenida de la MDK 8.2 va bastante mejor, aunque aun le queda para llegar al nivel del apt-get (Debian) o del emerge (Gentoo)

Presentacion de los servidores

Los dos demonios

Dos demonios se encargan de ofrecer los servicios de la conjunto de aplicaciones del Samba. El primero es el **smbd** y el segundo de ellos es el **nmbd**.

smbd es el demonio que se encarga de la comparticion de recursos: ficheros, impresoras, ... pero tambien del control del acceso a los recursos. Gestiona los permisos de los diferentes clientes una vez que estos han sido identificados.

El demonio **nmbd** se ocupa de anunciar servicios. Es decir, se encarga de informar a las maquinas presentes en la red sobre cuales son los recursos disponibles. Este demonio maneja tambien la resolucio de nombres de NetBIOS. Puede para ello comunicarse con un servidor WINS (Windows Internet Naming Service) presente en la red.

Nota : La resolucio de nombres consiste en obtener una equivalencia entre la direccio IP de la LAN y el nombre de la maquina.

Las herramientas de configuracion

Existen dos formas para realizar la configuracion:

Es posible editar directamente los ficheros de configuracion con un editor de texto, pero podemos configurar esos mismos ficheros con la ayuda de una interfaz gráfica, obteniendo identico resultado.

Nosotros veremos aquí el manejo de **Swat** (Samba Web Administration Tool). Se trata de una interfaz que se comporta como un servidor Web, conectandose a la maquina por medio de un simple navegador. Es posible leer la documentacion, cambiar la configuracion y realizar las demas tareas administrativas despues de habernos validado con un usuario y una contraseña.

Nota : El servidor Swat suele ejecutarse en el puerto 901, para no entrar en conflicto con el servidor de HTTP (Servidor Web) que suele escuchar el puerto 80.

Las herramientas del cliente

Las herramientas para el cliente bajo Microsoft Windows son aquellas utilizadas habitualmente para trabajar con servidores NT. No hay que cambiar nada en este sentido. El funcionamiento para las maquinas Windows es totalmente transparente.

Para GNU/Linux, existen en el paquete **samba-client** programas cliente para los servicios CIFS que sean proporcionados por un servidor Windows o por un servidor Unix usando Samba.

Configuracion con SWAT

La herramienta SWAT es el ejemplo de una buena interfaz de administracion grafica. Intenta de forma relativamente transparente poder proporcionar todas las funcionalidades de la configuracion en modo texto.

Nota : Como la configuracion de Samba es sencilla, ha sido posible agrupar todas las posibilidades en un numero reducido de opciones, sin sobrecargar la interfaz. Por otro lado SWAT ofrece la posibilidad de generar un fichero smb.conf de muestra, con el que podremos estudiar la sintaxis del script por si tuvieramos que editarlo a mano en alguna ocasión. De esta forma explicaremos las 2 formas de trabajar en paralelo

Presentacion de los ficheros en modo texto.

El fichero **/etc/smbpasswd** contiene los passwords de los usuarios de Samba, de forma cifrada.

El fichero **/etc/lmhosts** es un interfaz entre los nombres de maquinas NetBIOS y las direcciones IP numericas. Su formato es parecido al de **/etc/hosts**.

El fichero **/etc/smbusers** contiene una lista de usuarios del sistema, seguida de una lista de usuarios de Samba que disponen de los derechos de esos usuarios.

De esta forma es posible crear varios usuarios Samba sin tener que crear para cada uno de ellos un usuario del sistema.

Los menus de SWAT

Las secciones del **smb.conf**

Los menus **GLOBALS**, **SHARES**, **PRINTERS** son parecidos a los de las secciones existentes en el fichero **/etc/smb.conf**, que se presenta como un fichero **.ini** habitual del mundo Windows.

El menu **GLOBALS** contiene variables generales que se aplican al total de los recursos puestos a disposicion del servidor de SMB. Esta seccion contiene tambien informacion de identificacion del servidor dentro de la red NetBIOS: grupo de trabajo, nombre e identificador. Esta seccion contiene tambien los modos de funcionamiento de Samba.

El menu **SHARES** contiene la lista de comparticiones de disco efectuadas por la maquina. Se aconseja primero crear la particion compartida y despues precisar para cada particion sus propiedades particulares.

Nota: aquí hablo de particiones, pero tambien vale para carpetas/directorios compartidos.

El menu **PRINTERS** es casi identico al anterior, pero permite compartir impresoras en lugar de particiones de disco.

Los otros menus

El menu **HOME** permite acceder a la version HTML de la documentacion de Samba. Faltan talvez algunas opciones, en particular la ayuda sobre el propio SWAT deja algo que desear. Se trata a menudo de una ayuda relativa a las opciones de los ficheros en modo texto. A menudo más configurables que la herramienta grafica. De un modo u otro toda esta documentación es en el fondo muy usable.

El menu **VIEW** nos permite ver el fichero **smb.conf** tal cual ha sido redactado por SWAT. Es posible ver tambien la totalidad de las opciones posibles, incluso las que SWAT no ha cambiado, pero que tienen un valor por defecto.

El menu **PASSWORD** permite al usuario cambiar su contraseña. Se trata de un interfaz grafico para el programa **smbpasswd**. Sirve tambien al administrador para añadir nuevos usuarios.

Teoria de funcionamiento de CIFS

Anunciar los recursos disponibles

Sobre una misma red, varias maquinas pueden poner recursos a disposicion de otras. CIFS dispone de un

sistema para anunciar servicios (browsing), que permite saber que recursos compartidos hay disponibles.

Cada maquina que desea anunciar sus recursos compartidos a las otras maquinas contacta con una maquina en particular, la Servidora de Anuncios (Master Browser) que se encarga de centralizar estas notificaciones de presencia. Es posible configurar el servidor Samba para que sea el mismo Servidor de Anuncios o dejar esta tarea a una maquina Windows.

Restriccion de acceso a recursos

El acceso a los recursos puede controlarse de dos formas:

Escondiendo el recurso, es decir, no anunciandolo a ciertas maquinas de la red.

Estableciendo un sistema de validacion basado en contraseña, para restringir el acceso.

El anuncio de servicios esta limitado al "grupo de trabajo". Cada maquina Windows puede ser miembro de un solo grupo, y por tanto solo puede pertenecer a un conjunto de maquinas que compartan los mismos recursos. Es posible de este modo separar conjuntos de recursos compartidos, creando distintos grupos de trabajo. Si lo que deseamos es tener maquinas accediendo a los recursos de varios grupos distintos, es necesario pasar por un sistema de autentificacion.

Existen 4 formas distintas de autentificacion, cada una con sus ventajas e inconvenientes.

La autentificacion por usuario/contraseña.

Se trata del metodo por defecto. Representa la ventaja de permitir una gestion fina de los permisos. Para cada usuario es posible definir el acceso o no a unos recursos. Este metodo presenta un inconveniente: cada usuario debe disponer de una cuenta en la maquina Unix, para permitir la autentificacion.

El control de acceso por comparticiones.

Se trata de un metodo mas global: cada recurso compartido es protegido por un password propio. Para ello es necesario que varios usuarios conozcan el mismo password y que recuerden la contraseña adecuada para cada recurso compartido al que accedan.

Este metodo presenta la ventaja de que no son necesarias tantas cuentas de usuario como usuarios haya, sino tantas como recursos se compartan.

Autentificacion contra otro servidor.

Existen tambien dos metodos indirectos de control de acceso.

El primero, el metodo **server**, consiste en consultar con otro servidor CIFS, que se encargara de la autentificacion.

El segundo metodo, **domain**, consiste en validarse contra el servidor de dominio NT.

Nota : Un dominio NT es un conjunto de maquinas que comparten a la vez recursos y un proceso de autentificacion comun.

Configuracion de los parametros globales

Identificar el servidor

Primero hay que elegir algunos parametros de funcionamiento del servidor, para que se integre bien en la red.

El campo **server string**, permite elegir la descripcion que acompaña al nombre del servidor en la lista de recursos anunciados.

El campo **netbios name**, permite definir el nombre de la maquina, no como un nombre de DNS, sino como un nombre de resolucion de nombres propio del protocolo NetBIOS. Es importante entender que son dos cosas totalmente diferentes!

El campo **workgroup**, permite elegir el grupo de trabajo del que el servidor Samba hace parte.

El campo **interfaces** permite identificar la o las tarjetas de red que enlazan el servidor con el grupo de trabajo.

El control de acceso

El campo **security** permite elegir el metodo de autentificacion, podemos elegir uno de los vistos anteriormente.

Los menus **hosts allow** y **host deny** permiten controlar el acceso a los recursos de ciertas maquinas. Las configuraciones hechas en esta seccion se aplican a la totalidad de los recursos compartidos, independientemente de la configuracion especifica.

La seccion [GLOBAL]

Las configuraciones realizadas por Swat se reflejan en el fichero de configuracion /etc/smb.conf. Si editamos dicho fichero podremos ver algo de este estilo:

```
[global]
workgroup = nombre_del_grupo
server string = Servidor Samba
security = SHARE
log file = /var/log/samba/log.%m
max log size = 50
```

La comparticion de impresoras

Las ventajas de un servidor de impresion

Samba permite compartir facilmente una impresora conectada fisicamente a una maquina Unix, haciendo asi accesible a todas las maquinas conectadas a la red.

Una impresora de red que no soporte mecanismos de autentificacion puede ser puesta a disposicion de los usuarios gracias a un servidor de impresion de Samba, lo que permite controlar el acceso.

Utilizacion de la interfaz SWAT para configurar impresoras

Elegir la impresora

Esta operación se realiza dentro del menú **PRINTERS**. Este presenta una lista de impresoras existentes. Seleccionando una en la lista desplegable y usando el comando Choose Printer (elegir impresora) accederemos a su configuración.

Por defecto Samba extrae la lista de impresoras disponibles de **/etc/printcap**. Si la máquina dispone de otras impresoras, es posible añadirlas, introduciendo su nombre en el campo **Create Printer** y confirmando la acción.

Una lista de datos a rellenar aparece en este momento

El camino de acceso (PATH)

En el caso de una impresora se trata de del camino hacia el directorio utilizado por samba para conservar la cola de impresión. En general se adopta **/var/spool/samba**

Autorizar el acceso a invitados (guest)

Autorizar el acceso **guest**, es permitir a cualquier usuario de una máquina miembro del grupo de trabajo usar la impresora.

Atencion! La integración en un grupo de trabajo no es un método fiable de validación. Cualquier usuario de una máquina Windows puede cambiar su grupo de trabajo tantas veces como desee sin que ningún mecanismo de autenticación se lo impida. De este modo podría introducirse en un grupo con permisos de impresión un usuario al que en principio habíamos dejado fuera. Puede ser necesario usar restricciones por nombre de máquina (host allow, host deny) para una mayor seguridad

Anunciar el recurso

El menú browseable indica que este recurso debe ser anunciado por nmbd, y por tanto ser visible para todos los usuarios.

Compartición de directorios

Algunas opciones son idénticas a la compartición de impresoras.

Las opciones que permiten limitar el acceso a ciertas máquinas, elegir el camino de acceso al recurso (en este caso, directorio a compartir), y la autorización de un usuario invitado son idénticas a las que hemos encontrado en la sección PRINTERS

Afinando el control de acceso.

En el caso de la compartición de espacio en disco es posible tener un mejor control sobre el acceso.

Solo lectura

Es posible, activando la opción read only, autorizar solamente el acceso en modo lectura. Es posible definir sobre un mismo directorio varios tipos de permisos. Por ejemplo, se podría ofrecer acceso de solo lectura a la totalidad del grupo y luego afinar un acceso de escritura a ciertos usuarios en concreto.

Autenticaciones diversas

Si la seguridad está en modo compartido (share), todos los usuarios disponen, previa autenticación, de los derechos correspondientes al directorio que compartido. El sistema usa un método heurístico para determinar el identificador de un usuario que se conecta, pero este método es fácilmente manipulable. Así que más vale usar la autenticación en modo usuario, que permite por ejemplo compartir las carpetas personales del usuario sin riesgo alguno

La autenticación por cada usuario.

Las contraseñas encriptadas.

Por defecto, Samba no utiliza contraseñas cifradas. Esta elección le permite interoperar con clientes de Windows 3.x y Windows95

Pero por culpa de esta compatibilidad perdemos seguridad y es necesario tocar el registro del sistema de Windows en máquinas Win98 y posteriores para que todo funcione. Si en la red no hay máquinas windows95 o anteriores se aconseja configurar el servidor de Samba para que use contraseñas cifradas. Esto último se hace de esta forma, añadiendo en el fichero smb.conf la siguiente línea:

```
dentro del [global] de smb.conf :  
encrypt passwords = Yes
```

Estas contraseñas son almacenadas dentro del fichero `/etc/smbpasswd`. Las máquinas clientes contactan con el servidor y reciben una clave codificada usando la contraseña cifrada. El resultado es reenviado al servidor, que hace la misma operación. Si los dos resultados son idénticos la autenticación es correcta. Esto impide a un usuario "malicioso" hacerse con los passwords que atraviesan la red camino al servidor en busca de la autenticación.

Limitar el acceso a ciertos usuarios.

Para cada recurso es posible restringir el acceso a ciertos usuarios. Para cada una de las líneas de recursos compartidos en `/etc/smb.conf`, podemos añadir la línea :
valid users = usuario1, usuario2

En su ausencia, el recurso es accesible por todos los usuarios del servidor Samba. Si esta línea está presente el acceso está reservado únicamente a los usuarios mencionados.

Autorizar ciertos acceso en modo solo lectura

La opción **read only**, permite impedir a los usuarios que escriban en el directorio compartido. Podemos también limitar este acceso a unos usuarios concretos, para ello tenemos dos posibilidades :
Autorizar el acceso de escritura y bloquear ciertos usuarios con derecho de solo lectura, colocando su nombre en la sección **read list**= del recurso.

Autorizar el acceso en solo lectura y dar el privilegio de escritura a ciertos usuarios gracias a la seccion **write list**= del recurso compartido.

Integracion de Samba en un dominio NT

Los dominios NT

Los dominios NT son variantes de los grupos de trabajo. Igual que los grupos, permiten anunciar los recursos a diferentes clientes. La principal diferencia se encuentra a nivel de autentificacion. Todos los miembros de un dominio utilizan la misma base de datos de usuarios y contraseñas.

El metodo de autentificacion dentro de un dominio

Cuando un cliente miembro de un dominio intenta acceder a un recurso, envia una peticion a todas las maquinas de la red, y se autentifica contra la primera que responde. En una red NT, la tarea de responder se lleva a cabo la maquina "mas activa" que tenga acceso a la base de datos de usuarios. Se trata del **Primary Domain Controller (PCD)**, el controlador del dominio principal. En su ausencia, los servidores secundarios, los BCD pueden tomar el relevo.

Una vez la maquina cliente se ha autentificado con un controlador del dominio, el cliente no tiene porque volver a validarse dentro del dominio aunque decida acceder a otro recurso compartido diferente del inicial. El controlador del dominio "memoriza" las autentificaciones satisfactorias.

Utilizar un servidor NT para la autentificacion

Es posible configurar un servidor Samba para que se integre dentro de un dominio NT.

El primer paso consiste en declarar Samba como un miembro del grupo de trabajo del servidor NT. Seleccionando en el Swat **Security= SERVER**, le estamos pidiendo al servidor de Samba que contacte con un servidor NT (servidor NT indicado en la seccion `password server = nombre_del_servidor`) para la autentificacion. Evidentemene el servidor NT debe estar configurado para responder a las peticiones de autentificacion del servidor de Samba.

El siguiente paso es crear una cuenta para el servidor:

smbpasswd -j nombre_del dominio

Este es el metodo mas simple para integrar un servidor Samba en una red NT.

Por ultimo, hay que asegurarse de que cada usuario que el servidor NT va a autentificar tiene una cuenta en la maquina NT, para que los permisos funcionen.

Utilizar Samba como controlador del dominio

Si bien hace un tiempo esto no era oficial, Samba es actualmente totalmente capaz de comportarse como un PDC.

Configurar Samba como un PDC

Hay varias etapas.

1. Autorizar las peticiones de autentificación de otras maquinas.
2. Configurar la autentificación usuario por usuario
3. Declararse Master Browser, es decir invertir el mecanismo de eleccion habitual en las maquinas NT para llevarlas a nuestra maquina Samba.

La seccion [GLOBAL] debe contener los siguientes elementos:

```
domain logons = yes
security = user
os level = 34
local master = yes
preferred master = yes
domain master = yes
```

Configurar una comparticion permitiendo la autentificación

Creamos seguidamente una comparticion ficticia, siguiendo este patron :

```
[netlogon]
path = /export/samba/logon
public = no
writeable = no
browsable = no
```

Esta comparticion no ofrece el acceso a ningun recurso. Pero sin embargo permite la autentificación de diferentes maquinas.

Autorizar la conexión de las maquinas NT

Las maquinas NT intentan conectarse directamente al servidor, y no a un recurso en concreto. Es por tanto preciso autorizarlas para ello. Es necesario que las maquinas (y no los usuarios) dispongan de una cuenta. Las maquinas no van a conectarse al shell, asi que no es necesario darles un usuario del sistema con su directorio personal y demas.

El identificador de una maquina es su nombre NetBIOS, seguido del carácter \$. Asi por ejemplo la maquina iceberg, tendra como identificador iceberg\$. Hecho lo cual hay que añadir esta cuenta de usuario a la base de datos de los usuarios de Samba, con el comando :

```
smbpasswd -a -m maquina
```

Los clientes

Acceder a los recursos compartidos : smbclient

Este comando permite acceder, desde un cliente GNU/Linux, a recursos puestos a disposicion a traves de servidores CIFS, bien se trate de un servidor Samba o de un servidor basado en Microsoft Windows. La interfaz es parecida a la del ftp, es de este modo posible transferir ficheros sin esfuerzo. La sintaxis es :
smbclient [//maquina/recurso](#)

El recurso puede ser bien un directorio o bien una impresora, o un disco compartido al que se desea acceder. El nombre de la maquina es su nombre de NetBIOS, que puede (y suele) ser diferente de su nombre de DNS.

La opción -R permite elegir el modo de resolución del nombre de la máquina:

-R lmhosts permite consultar el fichero /etc/lmhosts, que resuelve nombres de IP contra nombres de NetBIOS de la máquina ,

-R wins permite lanzar la consulta a un servidor WINS para obtener dicha conversión.

Una vez conectado al servicio en cuestión, disponemos de una interfaz de transferencia de ficheros idéntica a la del FTP.

Disponemos de algunas opciones extra, tales como print fichero, para imprimir un fichero local en el servidor.

Integrar un recurso compartido en nuestra jerarquía de directorios: smbmount

El comando **smbmount** nos permitiera movernos de una manera más cómoda por los recursos compartidos vía CIFS. Se comporta de una forma similar a los montajes vía NFS: el recurso compartido CIFS se monta en un punto de nuestra jerarquía de directorios y podemos movernos por él usando los comandos Unix habituales. smbclient se encarga de gestionar las interacciones entre los ficheros presentes en el servidor.

Para desmontar un recurso compartido usamos el comando **smbumount**.

Guardar datos de un recurso compartido : smbtar

El comando smbtar es muy similar al comando tar. Permite realizar copias de seguridad de los archivos del servidor desde la máquina cliente Samba. La sintaxis es la siguiente:

smbtar -s servidor -x recurso -t lugar_de_almacenamiento

Nota: Es necesario disponer de permisos de lectura del directorio que deseamos almacenar. Es también posible crear copias incrementales con la opción -N fecha, que no almacena nada más que los ficheros que han sido modificados a partir de la fecha especificada.

Para profundizar ...

Referencias bibliográficas

- Eckstein Robert, et al. Using Samba. 1ª ed. O'Reilly & Associates, 1999. 416 pp. Collection O'Reilly System Administration. ISBN 1565924495. Una obra clara y completa sobre Samba. Desde su versión 2.07, este libro está disponible en HTML en los recursos de Samba y en PDF en Oreilly.com
- <http://www.samba.org/samba/docs/>. Documentación de Samba.

E-mail del autor: danirc@bulma.net

Podrás encontrar este artículo e información adicional en:
<http://bulmalug.net/body.phtml?nIdNoticia=1366>