Ficheros compartidos en red II: SAMBA.

Autor: Enrique V. Bonet Esteban

Introducción.

El servicio de SAMBA esta formado por un conjunto de aplicaciones que funcionan mediante el protocolo de aplicación SMB (Server Message Block)[1] y el protocolo de sesión NetBIOS. SMB/NetBIOS es un protocolo que utilizan sistemas operativos como Windows y OS/2 para operaciones de red entre clientes y servidores. Utilizando NetBIOS/SMB, un servidor de Linux puede colocarse en una red de ordenadores con sistema operativo Windows y actuar como servidor de los mismos, permitiendo:

- Compartir sistemas de archivos e impresoras.
- Autenticación y autorización de usuarios.
- Resolución de nombres en WINS.
- Anuncio de servicios.

Básicamente, el servicio de SAMBA funciona con dos programas, de nombres *smbd* y *nmbd*. El programa */usr/sbin/smbd* ofrece los servicios de acceso remoto a ficheros e impresoras y se encarga de autenticar y autorizar a los usuarios. Por su parte, el programa */usr/sbin/nmbd* realiza el anuncio del ordenador en el grupo de trabajo, la gestión de la lista de ordenadores de un grupo, etc., con lo que el sistema Linux aparece en la red como cualquier otro sistema Windows.

Adicionalmente, SAMBA posee algunas utilidades como *smbclient*, que permite conectarse desde Linux a recursos SMB y transferir ficheros, *smbtar*, que permite realizar copias de los recursos compartidos, *nmblookup*, que permite realizar búsquedas de nombres NetBIOS, *smbpasswd*, que maneja las claves encriptadas utilizadas por SAMBA, *smbstatus*, que informa de las conexiones de red existentes en los recursos compartidos por el servidor y *testparm*, que valida el fichero de configuración de SAMBA.

El servidor de SAMBA.

El servidor de SAMBA se arranca utilizando dos comandos:

```
systemctl start smb.service
```

[1] SMB también es conocido como Core Protocol, DOS Lan Manager, LAN Manager, NTLM (NT Lan Manager) y CISS (Common Internet File System), pues estos protocolos son SMB con pequeñas diferencias en su funcionalidad y/o implementación.

Que ejecuta el programa */usr/sbin/smbd*, el cual, como hemos comentado. es el que ofrece los servicios de acceso remoto a los recursos, y utiliza los puerto 139 TCP (*netbios-ssn*) y 445 TCP (*microsoft-ds*) para compartir los archivos[2].

Y el comando:

```
systemctl start nmb.service
```

Que ejecuta el programa */usr/sbin/nmbd*, que es el encargado de anunciar el ordenador en la red, etc., y que utiliza para ello los puertos 137 UDP (*netbios-ns*) y 138 UDP (*netbios-dgm*).

Es posible arrancar solo el servicio de smb, lo cual permitirá a SAMBA compartir archivos e impresoras, aunque no permitirá su anuncio en la red, etc., por lo que en tal caso sería necesario conocer previamente la existencia del recurso para poder utilizarlo.

La configuración de SAMBA, tanto servidor como cliente, se realiza en el fichero */etc/samba/smb.conf*. Este fichero establece las características de SAMBA y los recursos que se compartirán en la red. Aunque este fichero posee un gran número de opciones, la configuración del mismo suele ser sencilla, dado que el valor por defecto es apropiado para casi todas las opciones y casos posibles.

Como punto importante, resaltar que se consideran comentarios todas las líneas que comienzan por # y por ; (punto y coma), utilizándose generalmente el símbolo # para los comentarios formales y el punto y coma para comentar opciones de configuración. Además, el símbolo \ indica que la línea continúa en la línea siguiente, por lo que debe ignorarse el retorno de carro insertado a continuación.

De forma general, podemos considerar el fichero de configuración dividido en diferentes secciones. El comienzo de cada sección se indica mediante la etiqueta *[nombre de sección]*, siendo el final de una sección el comienzo de la siguiente. Por defecto, existen tres secciones especiales en el fichero de configuración de SAMBA y que son las secciones *[global]*, *[homes]* y *[printers]*.

La sección *[global]* define los parámetros de SAMBA del nivel global, así como los valores por defecto para el resto de parámetros en otras secciones si no se especifican en las mismas.

Por su parte, la sección *[homes]* define un recurso de red para cada usuario conocido por SAMBA y lo asocia al directorio raíz de cada usuario del ordenador servidor de SAMBA. Esta sección funciona como opción por defecto, pues un servidor SAMBA intenta primero comprobar si existe un servicio con ese nombre. Si no se encuentra, la solicitud se trata como un nombre de usuario y se busca en el fichero local de contraseñas. Si el nombre existe y la clave es correcta, se crea un servicio, cuyo nombre se cambia de *[homes]* al nombre local del usuario y, si no se especifica otro valor, se utiliza el directorio raíz del usuario.

[2] El puerto 139 es el utilizado por las versiones antiguas de Windows, mientras que el 445 es utilizado a partir de Windows 2000, aunque por compatibilidad, se puede seguir utilizando el puerto 139.

Por último, la sección *[printers]* define un recurso compartido para cada nombre de impresora conocida por SAMBA, que suelen ser las impresoras especificadas en el fichero */etc/printcap* del ordenador. Su funcionamiento es similar al de la sección *[homes]*[3].

Cualquier otro recurso (directorio o impresora) que se quiera compartir, debe especificarse creando una sección adicional en el fichero de configuración, donde el nombre de la sección se corresponderá con el nombre con el que el recurso será conocido en la red.

Las principales opciones de configuración de la sección global de SAMBA son[4]:

Opción	**Descripción**	**Valor por defecto**
workgroup	Nombre del grupo de trabajo o dominio de SAMBA.	Ninguno.
server string	Descripción del equipo en el dominio o grupo de trabajo.	Ninguno.
netbios name	Nombre del ordenador SAMBA.	Nombre DNS[5].
interfaces	Interfaces que utilizará SAMBA. Puede ser un interface (eth0), una dirección IP, una dirección IP/mascara o una dirección broadcast/mascara.	Todos los interfaces excepto el de loopback.
security	Nivel de seguridad[6].	user
passdb backend	Modo de almacenamiento de las contraseñas[7].	tdbsam
smb passwd file	Fichero con las contraseñas almacenadas.	En el ejecutable[8].
encrypt passwords	Utilizar contraseñas cifradas de Windows.	yes
password server	Servidores Windows para la autentificación.	Ninguno.
null password	Permitir el acceso de usuarios con contraseña nula.	no
map to guest	Indica cuando un acceso debe considerarse como invitado[9].	Never
hosts allow	Permite restringir los ordenadores y/o redes que pueden acceder al servidor.	Permiso a todos los ordenadores.
log file	Fichero de log	/var/log/samba/log.%m

[3] Si dos recursos compartidos de las secciones por defecto *[homes]* y *[printers]* tienen el mismo nombre, SAMBA es capaz de distinguir entre uno y otro por el tipo de mensaje de acceso al recurso, SMB_COM_OPEN para un directorio/fichero y SMB_COM_OPEN_PRINT_FILE para una impresora.

[4] Algunas de estas opciones pueden ser utilizadas en el resto de secciones para modificar el comportamiento por defecto del servidor en esa sección en particular.

[5] Por nombre DNS debe entenderse el primer componente del nombre DNS del ordenador, que generalmente corresponde al nombre del ordenador.

[6] Los niveles de seguridad se explican con posterioridad.

[7] Los posibles valores son smbpasswd, tdbsam y ldapsam, donde los dos primeros corresponden a almacenamientos locales y el último al uso de un servidor de ldap.

[8] La localización del fichero con la localización por defecto del fichero con las contraseñas almacenadas se realiza en la compilación del servidor de SAMBA. En la versión 17 de Fedora, el directorio es */var/lib/samba/private/passdb.tdb*

[9] Los valores posibles para este parámetro son Never (nunca), Bad User (el usuario no existe), Bad Password (el usuario existe pero la contraseña es incorrecta) y Bad Uid (cuando la autenticación es correcta pero no existe un usuario en Linux que corresponda al usuario Windows).

Opción	Descripción	Valor por defecto
max log file	Tamaño máximo del fichero de log.	50 KBytes.

Un sencillo ejemplo de sección *[global]* es el siguiente:

```
[global]
workgroup = ROBLIS
server string = SAMBA %v en %L
netbios name = glup
security = user
passdb backend = tdbsam
smb passwd file = /var/lib/samba/private/passdb.tdb
encrypt passwords = yes
map to guest = Never
hosts allow = 147.156.222. 147.156.223.
```

Donde %v se sustituye por la versión de SAMBA y %L por el nombre del ordenador SAMBA.

Por otra parte, las principales opciones de configuración del resto de secciones de SAMBA son:

Opción	Descripción	Valor por defecto
read only	Exportación del recurso en solo lectura.	yes
writeable	Exportación del recurso en modo escritura[10].	no
browseable	El servicio aparece en la lista de recursos en la red de Windows.	yes
path	Ruta absoluta al recurso	Ninguno.
comment	Descripción del servicio.	Ninguno.
guest ok	Permitir acceso como invitado.	no
guest account	Usuario que identifica el acceso como invitado.	nobody
guest only	Todos los accesos se realizan como invitado	no
force user	Fuerza a que el acceso al recurso se realice como el usuario especificado.	Ninguno.
force group	Fuerza a que el acceso al recurso se realice como el grupo especificado.	Ninguno.
hosts allow	Lista de ordenadores desde el que se permite el acceso.	Lista vacía (todos los ordenadores).
hosts deny	Lista de ordenadores a los que se les deniega el acceso.	Lista vacía (ningún ordenador).
printable	Indica si un dispositivo compartido es una impresora.	no
valid users	Lista de usuarios que pueden acceder al recurso.	Lista vacía (todos los usuarios).
follow symlinks	Permite el seguimiento de enlaces simbólicos	Yes

[10] read only y writeable se refieren al modo de exportación del recurso, solo que de forma inversa, así el equivalente de read only = yes es writeable = no.

Cuyo uso puede verse en el siguiente ejemplo, en el cual se exportan los directorios raíz de los usuarios:

```
[homes]
comment = Directorios raiz de los usuarios
browseable = yes
writeable = yes
```

O en este otro ejemplo, en el que se exportan las impresoras conectadas al servidor de SAMBA:

```
[printers]
comment = Impresoras
path = /var/spool/samba
browseable = no
guest ok = no
writeable = no
printable = yes
```

Un último ejemplo, en el que se exporta un directorio temporal para que los usuarios puedan escribir en el mismo, es el siguiente:

```
[tmp]
comment = Espacio temporal de disco
path = /tmp
browseable = yes
read only = no
guest ok = yes
```

Por último, comentar que SAMBA posee una serie de variables, que comienzan por el símbolo %, y que permiten especificar de forma variable distintos valores, como pueden ser un conjunto de directorios, etc. Las principales variables son:

Variable	**Definición**
%a	Arquitectura del cliente (SAMBA, WinNT, UNKNOWN, etc.)
%I	Dirección IP del cliente.
%m	Nombre NetBIOS del cliente.
%M	Nombre DNS del cliente.
%g	Grupo primario del usuario en Linux.
%G	Grupo primario del usuario que requiere el acceso.
%H	Directorio raíz del usuario en Linux.
%u	Usuario en Linux.
%U	Usuario que requiere el acceso.
%p	Directorio donde montar el recurso compartido.
%P	Directorio raíz compartido.
%S	Nombre del recurso compartido.
%d	Identificador del proceso.
%h	Nombre DNS del servidor
%L	Nombre NetBIOS del servidor.
%N	Directorio raíz del servidor.
%v	Versión de SAMBA.

Variable	Definición
%R	Versión del protocolo SMB.
%T	Día y hora actual del servidor.

Seguridad en el servidor de SAMBA.

Una de las consideraciones más importantes a la hora de configurar SAMBA es la selección del nivel de seguridad. Su selección se realiza con la opción *security*, de la sección *[global]*. Dicha opción puede tomar los valores *share*, *user*, *server* y *domain*, aunque los valores *share* y *server* son obsoletos pero se pueden seguir utilizando por compatibilidad.

El valor *share* especifica que cada recurso posee una contraseña asociada, de forma que un cliente debe proporcionar dicha contraseña cada vez que pide una conexión al recurso compartido por SAMBA. Este valor suele utilizarse en dominios en que todavía existan ordenadores con sistemas operativos Windows 95/98/Millenium, en los que cada recurso tiene asignada su propia contraseña para acceder por la red.

Por otro lado, los valores *user*, *server* y *domain* indican que la validación se realice a nivel de usuario y no de recurso, de forma que el usuario, una vez autentificado, puede acceder a los recursos a los que tuviera permiso de forma local, sin necesidad de proporcionar una contraseña para acceder a cada uno de ellos. La diferencia entre los valores *user*, *server* y *domain* se encuentra en como se realiza la autentificación.

El valor *user* especifica que la validación la realiza el sistema Linux donde SAMBA se ejecuta, de forma similar a la que se realizaría si el usuario iniciase una sesión local en el ordenador. Para que este método sea aplicable, es necesario que existan los mismos usuarios y con idénticas contraseñas en los sistemas Windows y Linux donde SAMBA se ejecuta. Además, desde Windows NT 4.0 (a partir del Service Pack 3), y sistemas Windows posteriores, la utilización del valor *user* es problemático debido a que estos sistemas Windows transmiten, por defecto, las contraseñas cifradas por la red. Como SAMBA no posee acceso a las contraseñas cifradas por Windows, el sistema Linux no puede realizar la validación de forma normal, lo que obliga a modificar el registro del sistema Windows para que transmita las contraseñas sin cifrar o bien, a utilizar una tabla de contraseñas adicional en Linux, la cual debe almacenar las contraseñas cifradas de los usuarios de los sistemas Windows[11].

El valor domain establece que SAMBA realice la validación del usuario en un servidor de dominio de Windows, generalmente un Windows 2003 o Windows 2008[12]. Cuando un cliente intenta iniciar una sesión con SAMBA, éste intenta iniciar una sesión con el ordenador en el que ha delegado la validación de la acreditación mediante el usuario y contraseña recibidos del cliente. Si la apertura de sesión realizada por

[11] Con posterioridad, veremos con más detalle este método de autentificación en SAMBA.

[12] Este método implica que el servidor de SAMBA es un miembro del dominio de Windows, con lo que puede utilizar las relaciones de confianza existentes en el dominio de Windows, de forma que usuarios de otros dominios en los que los controladores de dominio de Windows confían, son validados para su acceso al servidor de SAMBA.

SAMBA es correcta, la solicitud del cliente es aceptada, siendo denegada en caso contrario.

Este método proporciona la ventaja de no necesitar que las contraseñas sean las mismas en los sistemas Windows y Linux, así como el permitir el envío de contraseñas cifradas de Windows, dado que la autentificación se realiza en un servidor de Windows. Además, este método requiere crear un usuario en el ordenador servidor de SAMBA para poder efectuar ciertas operaciones de entrada/salida que requieren la existencia de un usuario. La forma normal de realizarlo es creando una cuenta de usuario y deshabilitar la misma en la tabla de contraseñas de acceso al sistema, pues el usuario nunca accederá al sistema mediante su identificándose.

Para el valor del valor obsoleto *server*, la autentificación es similar a la del valor *domain*, excepto que en este caso la validación se delega en un ordenador cualquiera que ejecute el sistema operativo Windows, y no en un servidor de dominio.

Autentificación mediante user.

Como hemos visto, el valor *user* en el nivel de seguridad especifica que la validación se realiza en el servidor Linux donde se encuentra SAMBA. Además, hemos visto que es posible, modificando el registro de los sistemas Windows, permitir el envío de contraseñas sin cifrar. Sin embargo, y dado el peligro que supone el envío de contraseñas sin cifrar, veremos con detalle como configurar SAMBA para que sea capaz de aceptar contraseñas cifradas.

Para ello, lo primero que debemos realizar es crear el fichero con las contraseñas cifradas en el servidor SAMBA. Supondremos que hemos elegido la opción de almacenar las contraseñas como *tdbsam*, con lo que los ficheros por defecto donde se almacenan los datos son */var/lib/samba/private/passdb.tdb*, y */var/lib/samba/private/secrets.tdb*. Estos ficheros suelen venir ya creados en la instalación del sistema, con lo que deberemos proceder a introducir los usuarios que existan en el sistema. El manejo de los usuarios de SAMBA se realiza con el comando */usr/bin/smbpasswd*, cuyas principales opciones son:

Opción	**Descripción**
-a	Añade un usuario y su contraseña a SAMBA o modifica su contraseña si el usuario ya existe. El usuario debe existir como usuario de Linux para poder ser añadido a SAMBA.
-x	Elimina un usuario de SAMBA.
-d	Deshabilita la cuenta de un usuario de SAMBA.

Opción	Descripción
-e	Habilita la cuenta de un usuario de SAMBA.
-n	Asigna un password nulo al usuario especificado. El usuario solo podrá acceder si se ha permitido en la sección global la validez de los passwords nulos.

Así, si deseamos añadir un nuevo usuario a SAMBA ejecutaremos el comando:

```
/usr/bin/smbpasswd -a <usuario>
```

Introduciendo el nuevo usuario y solicitando la contraseña del mismo.

La autenticación mediante *user* posee el problema de que cada cambio de la contraseña de un usuario en Windows, debe realizarse en el servidor de SAMBA. Además, las contraseñas de un usuario pueden ser distintas en el fichero de contraseñas de SAMBA y en el fichero de contraseñas de acceso al sistema, lo que dificulta aún más su mantenimiento.

Para evitar esto último, SAMBA posee mecanismos de sincronización entre el fichero de claves de acceso al sistema[13] ambos ficheros de contraseñas. La forma más sencilla de llevar a cabo esta sincronización es introduciendo, en la sección global de configuración del servidor, los valores:

```
unix password sync = yes
passwd program = /usr/bin/passwd %u
```

Donde el primer valor especifica que se sincronicen las contraseñas, indicando el segundo valor el programa a ejecutar para modificar las contraseñas en el fichero de acceso al sistema[14].

El cliente de SAMBA.

Como hemos visto, el servidor de SAMBA posee cuatro mecanismos diferentes de autentificar los clientes. Sin embargo, desde el punto de vista de un cliente, solamente existen dos mecanismos diferentes, los denominados *share* y *user*, pues el modo *user* en el cliente recoge los modos *user*, *server* y *domain* del servidor.

En efecto, un cliente SAMBA solo necesita conocer si debe enviar una contraseña al servidor para acceder al dispositivo (modo de autentificación *share*) o bien, debe enviar un usuario y contraseña al servidor (modos de autentificación *user*, *server* y *domain*), pues para el cliente es independiente de si la autentificación la realiza el propio servidor SAMBA (modo *user*), otro ordenador (modo *server*) o un servidor de dominio (modo *domain*).

En el modo *share*, la protección del acceso al recurso recae en una contraseña que asociamos al mismo, de forma que un usuario de un cliente debe proporcionar dicha

[13] Las contraseñas del sistema se encuentran en /etc/passwd y /etc/shadow si el sistema ha sido habilitado en modo de contraseñas “shadow”.
[14] La opción %u indica a SAMBA que se sustituya su valor por el nombre del usuario.

contraseña para acceder al recurso. Una vez se ha accedido al recurso, no existe ninguna restricción en el uso del mismo. Este es el método de autentificación de SMB para los Windows 95/98/Millenium.

En el modo *user*, el servidor recibe del cliente una credencial de usuario (nombre, dominio y contraseña) que debe autentificar para permitir el acceso al recurso. Una vez accedido al recurso, el uso que el cliente puede hacer del mismo depende de la autentificación recibida, de forma que no todos los usuarios pueden ejecutar todas las acciones sobre el cliente. Este modo es el método de autentificación de SMB en sistemas Windows NT, 2000, XP, etc.

Además de lo anterior, en el fichero de configuración de SAMBA, que como hemos indicado con anterioridad es */etc/samba/smb.conf*, podemos especificar los modos permitidos de envío de contraseñas del cliente al servidor. Esto se indica con la opción:

```
client {plaintext | lanman | ntlmv2} auth = {yes|no}
```

Donde *plaintext* indica que se permite el envío de contraseñas en modo texto sin cifrar, *lanman* indica que se permite el envío de contraseñas cifradas con LANMAN[15] y *ntlmv2* indica que se permite el envío de contraseñas cifradas con NTLMv2. Si no se indica ningún tipo de cifrado, el cliente utiliza por defecto NTLMv2.

Como comentario adicional, aunque en un fichero de configuración se active explícitamente más de un tipo de cifrado, solo se utilizará el modo de cifrado más seguro, quedando el resto de cifrados desactivados automáticamente al especificar explícitamente un cifrado más seguro.

Como es obvio, existen clientes de SAMBA tanto en Linux como en Windows, centrándonos brevemente en la descripción del cliente Linux[16].

El cliente Linux de SAMBA es una utilidad incluida en la distribución del servidor de SAMBA y que se denomina *smbclient*. El programa *smbclient* se encuentra en */usr/bin/smbclient* y, aunque posee un gran número de opciones, su ejecución básica obedece a la siguiente sintaxis:

```
/usr/bin/smbclient <recurso compartido> [clave] [-U usuario]
```

Donde <*recurso compartido*> es el nombre del recurso compartido al que se desea acceder, siendo la forma de expresarlo igual a como se realiza en Windows, esto es:

```
//<nombre NetBIOS>/<recurso>
```

Donde <*nombre NetBIOS*> es el nombre NetBIOS del ordenador que posee el recurso al que queremos conectarnos, y <*recurso*> es el nombre del recurso solicitado.

[15] LANMAN es un cifrado fácil de romper pues el algoritmo es débil y no distingue entre mayúsculas y minúsculas.

[16] El cliente Windows de SAMBA es un cliente Windows cualquiera que pueda ser utilizado para conectarse a cualquier recurso compartido de Windows, por lo que no será explicado en estos apuntes.

El parámetro *[clave]* es opcional, y corresponde a la contraseña del usuario con el que queremos conectarnos al recurso. Si no se facilita ninguna contraseña, esta será solicitada por el programa en el momento de establecer la conexión con el servidor del recurso compartido.

Por último, el parámetro *[-U usuario]* permite especificar el nombre del usuario con el que nos conectaremos al recurso compartido, pues en caso de no ser especificado, el usuario que se envía es el nombre del usuario de Linux que ejecuta el comando *smbclient*.

Una vez conectados, la desconexión se lleva a cabo sencillamente ejecutando el comando *quit* en el interfaz del recurso compartido.

Como comentario final, un ordenador Windows puede funcionar como cliente de un servidor de SAMBA de forma similar a la vista con anterioridad para Linux. Además de las opciones gráficas que posee Windows, podemos ejecutar comandos similares a los de Linux. Por ejemplo, para montar un recurso SAMBA en Windows podemos ejecutar el comando:

```
net use {unidad|*} <recurso compartido> [clave] [/u:<usuario>]
```

Donde unidad indica la unidad donde se conectará el recurso compartido, pudiendo especificarse mediante * la primera unidad libre, siendo el resto de parámetros similares a los explicados para Linux[17].

Si lo que deseamos es desconectarnos en Windows de una unidad compartida, podemos ejecutar el comando:

```
net use <unidad> /delete
```

Donde <*unidad*> es la unidad donde fue montado el recurso compartido.

Ejercicios.

1- Deseamos configurar un ordenador de forma que permita compartir una impresora mediante SAMBA, con el nombre *impcom*, para ordenadores Windows 95/98/Millenium. Escribir el fichero de configuración necesario.

2- Deseamos compartir los directorios de los usuarios de un ordenador de forma que otros ordenadores Windows NT/2000/XP tengan acceso a los mismos mediante SAMBA, pero solo en modo de lectura. Escribir el fichero de configuración que responda a estos requisitos.

3- Un ordenador posee un directorio */var/ftp/pub*, el cual deseamos compartir con otros ordenadores, con el nombre publico, mediante SAMBA, en modo de lectura y escritura y para todo tipo de ordenadores Windows (95/98/Millenium/NT/2000/XP). Escribir el fichero de configuración necesario.

[17] El recurso compartido se especifica como \\<*nombre NetBIOS*>\<*recurso*>.