

Configuración de Samba

Indice:

1.- <i>¿Qué es Samba?</i> _____	1
2.- <i>Instalación de Samba.</i> _____	2
3.- <i>Configuración de Samba.</i> _____	3
4.- <i>Instalación/Configuración de swat.</i> _____	4
5.- <i>Niveles de seguridad</i> _____	5
6.- <i>Configuración de Samba con el nivel de seguridad domain.</i> _____	6
7.- <i>Tratamiento de los accesos como invitado</i> _____	7
8.- <i>El sistema de ficheros SMB para linux</i> _____	7
9.- <i>Opciones del servidor Samba</i> _____	8
10.- <i>Opciones del recurso</i> _____	8

1.- ¿Qué es Samba?

Samba es un producto¹ que se ejecuta en sistemas Unix, permitiendo al sistema Unix *conversar* con sistemas Windows a través de la red de forma nativa. De esta forma, el sistema Unix aparece en el “Entorno de red”, y clientes Windows pueden acceder a sus recursos de red e impresoras compartidas como si de otro sistema Windows se tratase. Para ello, Samba implementa los protocolos NetBIOS y SMB. NetBIOS es un protocolo del nivel de sesión que permite establecer sesiones entre dos ordenadores. SMB (Server Message Block), implementado sobre NetBIOS, es el protocolo que permite a los sistemas Windows compartir ficheros e impresoras.

Esencialmente, Samba consiste en dos programas, denominados `smbd` y `nmbd`. Ambos programas utilizan el protocolo NetBIOS para acceder a la red, con lo cual pueden conversar con ordenadores Windows. Haciendo uso de estos dos programas, Samba ofrece los siguientes servicios, todos ellos iguales a los ofrecidos por los sistemas Windows:

- Servicios de acceso remoto a ficheros e impresoras.
- Autenticación y autorización.
- Resolución de nombres.
- Anuncio de servicios.

¹ Samba se distribuye gratuitamente para varias versiones de Unix, de acuerdo con los términos de la General Public License de GNU.

El programa `smbd` se encarga de ofrecer los servicios de acceso remoto a ficheros e impresoras (implementando para ello el protocolo SMB), así como de autenticar y autorizar usuarios. `smbd` ofrece los dos modos de compartición de recursos existentes en Windows, basado en usuarios o basado en recursos. En el modo basado en usuarios (propio de los dominios NT) la autorización de acceso al recurso se realiza en función de nombres de usuarios registrados en un dominio, mientras que en el modo basado en recursos (propio de Windows 3.11) a cada recurso se le asigna una contraseña, estando autorizado el acceso en función del conocimiento de dicha contraseña.

El programa `nmbd` permite que el sistema Unix participe en los mecanismos de resolución de nombres propios de Windows, lo cual incluye el anuncio en el grupo de trabajo, la gestión de la lista de ordenadores del grupo de trabajo, la contestación a peticiones de resolución de nombres y el anuncio de los recursos compartidos. De esta forma, el sistema Unix aparece en el “Entorno de Red”, como cualquier otro sistema Windows, publicando la lista de recursos que ofrece al resto de la red.

Adicionalmente a los dos programas anteriores, Samba ofrece varias utilidades. Algunas de las más relevantes son las siguientes:

- `smbclient` . Una interfaz similar a la utilidad `ftp`, que permite a un usuario de un sistema Unix conectarse a recursos SMB y listar, transferir y enviar ficheros.
- `swat` . Samba Web Administration Tool. Esta utilidad permite configurar Samba de forma local o remota utilizando un navegador de web.
- Sistema de ficheros SMB para Linux. Linux puede montar recursos SMB en su jerarquía, al igual que sucede con directorios compartidos vía NFS.

2.- Instalación de Samba.

Los pasos que hay que seguir para instalar Samba en RedHat Linux son los siguientes:

- 1) Montar el directorio `/espacio/raiz/home/ftp/pub` de `adserver` en el directorio local `/mnt`
- 2) Cambiar al directorio `/mnt/Redhat6.0/RedHat/RPMS` para iniciar la instalación.
- 3) Instalar Samba:
`rpm -ih Samba-2.0.3-8.i386.rpm`
- 4) Actualizar Samba:
`cd ../../updates/`
`rpm -Uh Samba-2.0.5a-1.i386.rpm`
`rpm -Uh Samba-client-2.0.5a-1.i386.rpm`

Una vez instalado Samba, hay que verificar que el servicio `smb` está activo en el niveles de ejecución 3 y/o 5 y reiniciar el sistema.

3.- Configuración de Samba.

La configuración de Samba se realiza en el fichero `/etc/smb.conf`. En este fichero se establecen las características del servidor Samba, así como los recursos que serán compartidos en la red. La utilización de este fichero es bastante sencilla, ya que aunque existe un gran número de opciones, muchas de ellas pueden obviarse dado que siempre existe un valor por defecto para cada opción, que suele ser apropiado. A título de ejemplo, a continuación se muestra un fichero de configuración simple, que exporta el directorio de conexión de cada usuario como un recurso de red distinto y el directorio `/espacio/pub` como el recurso de red `pub`.

```
[global]
...
[homes]
    comment = Home Directories
...
[pub]
    path = /espacio/pub
```

Como se ve en el ejemplo, el fichero `/etc/smb.conf` se encuentra dividido en secciones, encabezadas por una palabra entre corchetes. Dentro de cada sección figuran opciones de configuración, de la forma “etiqueta = valor”, que determinan las características del recurso exportado por la sección. En los apartados 8 y 9 del presente documento se citan las opciones más importantes que se pueden establecer en cada sección.

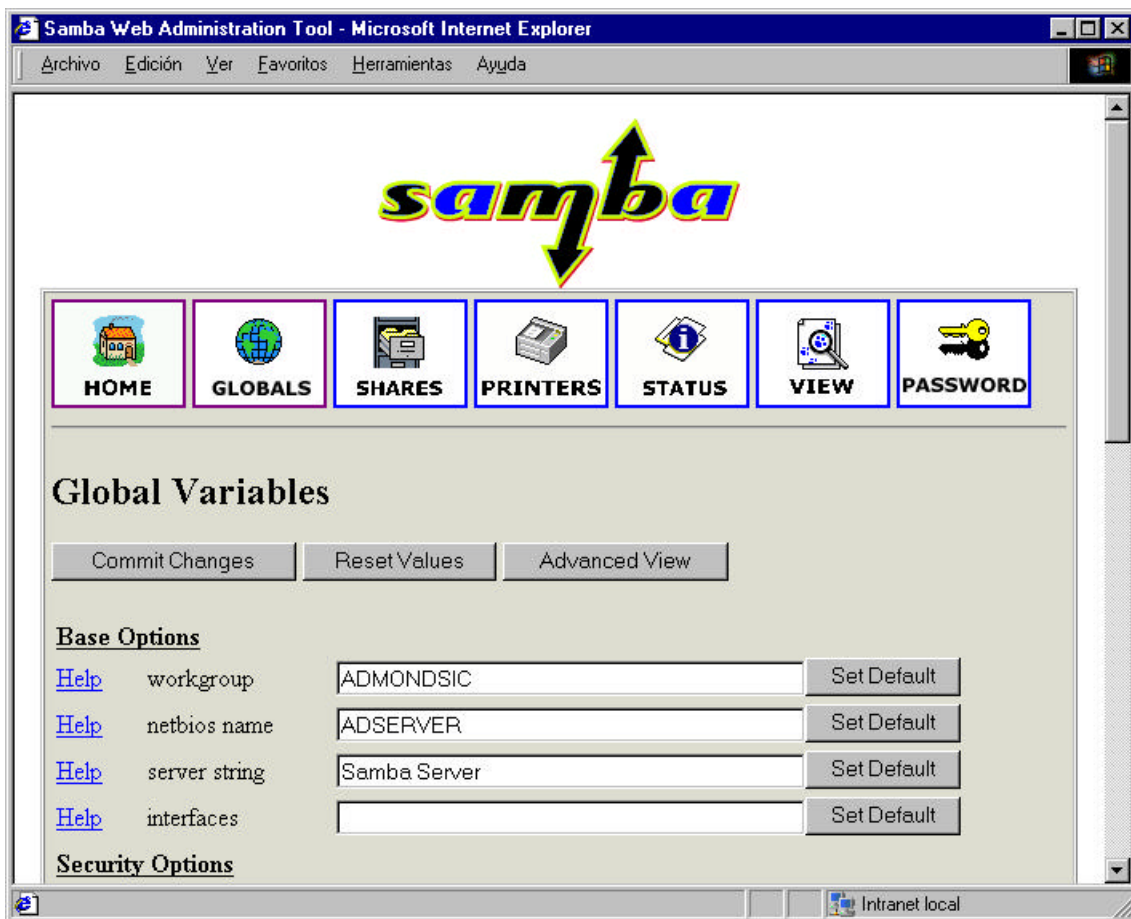
Existen tres secciones predefinidas, denominadas `global`, `homes` y `printers`, y tantas secciones adicionales como recursos extra se quieran compartir. Las secciones predefinidas tienen el siguiente cometido:

[global]	Define los parámetros de Samba a nivel global del servidor, así como los parámetros que se establecerán por defecto en el resto de las secciones.
[homes]	Define automáticamente un recurso de red por <i>cada</i> usuario conocido por Samba. Este recurso, por defecto, está asociado al directorio de conexión de cada usuario en el ordenador en el que Samba está instalado.
[printers]	Define un recurso compartido por cada nombre de impresora conocida por Samba.

Para cualquier otro recurso (directorio o impresora) que se quiera compartir hay que definir una sección adicional en el fichero de configuración. El encabezamiento de

dicha sección (pub en el ejemplo anterior) corresponderá al nombre que el recurso tendrá en la red.

Por otra parte, Samba ofrece una interfaz de edición de este fichero basada en web denominada *swat*. Esta herramienta permite configurar Samba utilizando un navegador de red, tanto de forma local como remota. El aspecto de esta interfaz es el siguiente:



4.- Instalación/Configuración de swat.

swat es un programa que atiende peticiones http en el puerto tcp 901. Para activar *swat* es necesario seguir los pasos siguientes

- 1) Declarar el servicio *swat*.

Incluir en el fichero `/etc/services` la siguiente línea:

```
swat 901/tcp
```

- 2) Asociar el programa *swat* al nuevo servicio.

En el fichero `/etc/inetd.conf` incluir la siguiente línea:

```
swat stream nowait.400 root /usr/local/Samba/bin/swat swat
```

- 3) Activar el servicio *swat*.

```
/etc/rc.d/init.d/inet restart
```

A partir de este momento, la configuración de Samba puede realizarse vía Web. Para ello, basta con acceder a la dirección `http://nombre_de_ordenador:901/`

5.- Niveles de seguridad

Una de las consideraciones más importantes a la hora de configurar Samba es la selección del nivel de seguridad.

Desde la perspectiva de un cliente, Samba ofrece dos modos de seguridad, denominados `share` y `user`, al igual que sucede en los sistemas Windows:

- En el modo `share`, cada vez que un cliente quiere utilizar un recurso ofrecido por Samba, debe suministrar una contraseña de acceso asociada a dicho recurso.
- En el modo `user`, el cliente debe establecer en primer lugar una sesión con el servidor Samba, para lo cual le suministra un nombre de usuario y una contraseña. Una vez Samba valida al usuario, el cliente obtiene permiso para acceder a los recursos ofrecidos por Samba.

En cualquiera de ambos, Samba tiene que asociar un usuario del sistema Unix en el que se ejecuta Samba con la conexión realizada por el cliente. Este usuario es el utilizado a la hora de comprobar los permisos de acceso a los ficheros y directorios que el sistema Unix/Samba comparte en la red.

La selección del nivel de seguridad se realiza con la opción `security`, la cual pertenece a la sección `[global]`. Sus alternativas son las siguientes:

```
security = share | user | server | domain
```

Desde la perspectiva del cliente, el nivel `share` corresponde al modo de seguridad `share` y los niveles `user`, `server` y `domain` corresponden todos ellos al modo de seguridad `user`. A continuación se describen someramente los cuatro niveles.

El nivel `share` es utilizado normalmente en entornos en los cuales no existe un dominio NT, dado que es complejo y costoso el mantenimiento de una tabla de usuarios global para la red.

En el nivel `user`, el encargado de validar al usuario es el sistema Unix donde Samba se ejecuta. La validación es idéntica a la que se realizaría si el usuario iniciase una sesión local en el ordenador Unix. Para que este método sea aplicable, es necesario que existan los mismos usuarios y con idénticas contraseñas en los sistemas Windows y en el sistema Unix donde Samba se ejecuta.

Recientemente, la utilización de este nivel se ha vuelto complicada, ya que en Windows 98 y en Windows NT (Service Pack 3 y posteriores), las contraseñas de los usuarios se

transmiten cifradas por la red. Puesto que el tipo de cifrado no es conocido por Samba, el sistema Unix ya no puede realizar la validación. Existen dos métodos para resolver este problema. El primero consiste en modificar el registro del sistema Windows para permitir la transferencia de contraseñas sin cifrar por la red. El segundo método obliga a utilizar una tabla de contraseñas adicional en el sistema Unix, en la cual se almacenan las contraseñas cifradas de los usuarios Windows.

En el nivel `server`, Samba delega la validación del usuario en otro ordenador, normalmente un sistema Windows NT. Cuando un cliente intenta iniciar una sesión con Samba, éste último intenta iniciar una sesión en el ordenador en el cual ha delegado la validación con la misma acreditación (usuario+contraseña) recibidos del cliente. Si la sesión realizada por Samba es satisfactoria, entonces la solicitud del cliente es aceptada. Este método aporta la ventaja de no necesitar que las contraseñas se mantengan sincronizadas entre los sistemas Windows y Unix, ya que la contraseña Unix no es utilizada en el proceso de validación. Adicionalmente, no hay inconveniente en utilizar contraseñas cifradas, ya que la validación la realiza un sistema NT.

Por último, existe la posibilidad de utilizar el nivel `domain`. Este nivel es similar al nivel `server`, aunque en este caso el ordenador en el que se delega la validación debe ser un PDC (o una lista de ordenadores PDC y BDC). La ventaja de este método estriba en que el ordenador Samba pasa a ser un verdadero miembro del dominio NT, lo que implica, por ejemplo, que puedan utilizarse las relaciones de confianza establecidas por el dominio. Esto significa, en pocas palabras, que usuarios pertenecientes a otros dominios en los que el PDC confía son conocidos por Samba. Por otra parte, como comentan los creadores de Samba, este método permitirá en un futuro cercano eliminar la necesidad de mantener una tabla de usuarios en el sistema Unix sincronizada con la tabla de usuarios del dominio NT. En fin, tal como dicen ellos, “*watch for this code soon!*”.

Dadas las ventajas de el nivel `domain`, este documento se centra fundamentalmente en este método. Para detalles específicos de los otros niveles, se recomienda la consulta de la documentación original de Samba.

6.- Configuración de Samba con el nivel de seguridad `domain`.

Los pasos a seguir para configurar Samba con el nivel de seguridad `domain` son los siguientes:

- 1) Dar de alta en el PDC al sistema Unix donde se ejecuta Samba como miembro del dominio. Esta acción se realiza desde el “Administrador de Servidores”
- 2) Detener el servidor Samba
`/etc/rc.d/init.d/smb stop`
- 3) Agregar el sistema Unix al dominio.
`smbpasswd -j DOMINIO -r PDC_DEL_DOMINIO`
- 4) Configurar el nivel en el fichero `/etc/smb.conf`.
En la sección `[global]` incorporar:
`security = domain`
`workgroup = DOMINIO`

```
encrypt passwords = yes
password server = PDC_DEL_DOMINIO
```

- 5) Iniciar el servidor Samba
`/etc/rc.d/init.d/smb start`

7.- Tratamiento de los accesos como invitado

Cuando se utiliza el nivel de seguridad `domain`, el tratamiento de los accesos como usuario invitado requiere algunas consideraciones.

En primer lugar, Samba considera a un usuario como invitado sólo cuando este usuario está dado de alta en el dominio NT al cual pertenece Samba pero no está dado de alta en el sistema Unix donde Samba se ejecuta. De esta forma, usuarios de otros dominios (en los que *no* se confía) no pueden acceder a Samba, ni siquiera como invitados.

Para conseguir que usuarios ajenos al dominio NT se consideren invitados, es necesario activar la siguiente opción en la sección `[global]` :

```
map to guest = Bad User
```

De esta forma, cualquier usuario no conocido será tratado como invitado. Samba considerará que los accesos al sistema de ficheros Unix los realizará el usuario especificado en la opción global `guest account`. En cualquier caso, el acceso como invitado debe permitirse expresamente para cada recurso con la opción `guest ok`.

8.- El sistema de ficheros SMB para linux

Linux dispone de soporte para el sistema de ficheros SMB. De esta forma, Linux, al igual que puede montar un directorio exportado vía NFS en un directorio local, puede montar un recurso SMB ofrecido por un servidor SMB (Un sistema Windows o un servidor Samba, por ejemplo).

No obstante, existe una diferencia significativa entre NFS y SMB. En NFS no se requiere autenticar al usuario que realiza la conexión; el servidor NFS utiliza el UID del usuario del ordenador cliente para acceder a los ficheros y directorios exportados. Un servidor SMB, por contra, requiere autenticar al usuario, para lo que necesita un nombre de usuario y una contraseña. Por ello, para montar un recurso SMB se utiliza un mandato específico, denominado `smbmount`, cuya utilización es la siguiente:

```
smbmount '//ordenador/recurso' directorio_local -U nombre_de_usuario -W
grupo_de_trabajo_o_domino
```

Tras ejecutar este mandato se requiere la introducción de la contraseña. Si el servidor SMB valida al usuario, a partir del directorio `directorio_local` se consigue el acceso al recurso `//ordenador/recurso`.

El recurso puede desmontarse utilizando el mandato `smbumount` , cuya utilización es la siguiente:

```
smbumount directorio_local
```

9.- Opciones del servidor Samba

A continuación se describen algunas opciones del servidor Samba. Estas opciones tan sólo son aplicables a la sección `[global]`.

Opción	Significado	Valor por defecto
<code>netbios name</code>	Nombre NetBIOS del ordenador	Primer componente de su nombre DNS.
<code>log level</code>	Detalle en la auditoría de Samba. Es un número que indica la cantidad de información a auditar. A mayor valor, más cantidad de información.	Se establece en el script que inicia el servicio Samba
<code>log file</code>	Nombre del fichero donde se almacenan los mensajes de auditoría de Samba	Se establece en el script que inicia el servicio Samba
<code>wins server</code>	Ordenador servidor de WINS. El sistema Samba se convierte en cliente WINS.	nulo
<code>wins support {yes/no}</code>	El ordenador Samba se convierte en servidor WINS (funcionalidad limitada).	no

10.- Opciones del recurso

A continuación se describen algunas opciones aplicables a cada recurso compartido. Pueden establecerse también en la sección global, siendo en este caso utilizadas como valores por defecto para cada recurso compartido.

Opción	Significado	Valor por defecto
<code>read only {yes/no}</code>	Recurso de solo lectura	yes
<code>browseable {yes/no}</code>	El servicio aparece en la lista de recursos compartidos	yes
<code>path</code>	Directorio asociado al servicio	--
<code>comment</code>	Descripción del servicio	--

guest ok {yes no}	Permitir los accesos en modo invitado.	no
guest account	Si un acceso se realiza como invitado (usuario no conocido), se utiliza el usuario especificado para representar la conexión	nobody
guest only	Cualquier acceso se realiza en modo invitado.	no
copy	Duplica un servicio ya declarado	
force user	Los accesos al recurso se realizan como si el usuario que accede es el usuario indicado	Se utiliza el mismo usuario que ha realizado la conexión
force group	Los accesos al recurso se realizan como si el usuario pertenece al grupo indicado	Se utiliza el grupo primario del usuario que ha realizado la conexión
hosts allow	Lista de ordenadores a los que se les permite acceder	lista vacía (i.e., todos los ordenadores)
hosts deny	Lista de ordenadores a los que no se les permite acceder. En caso de conflicto, prevalece lo indicado en hosts allow	ningún ordenador
valid users	Lista de usuarios que pueden acceder a este recurso	lista vacía (i.e., todos los usuarios)
follow symlinks {yes/no}	Permitir el seguimiento de los enlaces simbólicos.	yes