

Cómo configurar SAMBA.

Autor: Joel Barrios Dueñas

Correo electrónico: [joelbarrios arroba linuxparatodos punto net](mailto:joelbarrios@linuxparatodos.punto.net)

Sitio de Red: <http://www.linuxparatodos.net/>

Jabber ID: darkshram@jabber.org

Usted puede contribuir financiando la elaboración de más documentos como éste haciendo aportaciones voluntarias y anónimas en:

HSBC (México)

Cuenta: 4007112287, Sucursal 00643

A nombre de: Joel Barrios Dueñas.

Creative Commons [Reconocimiento-NoComercial-CompartirIgual 2.1](https://creativecommons.org/licenses/by-nc-sa/2.1/)

© 1999-2005 Linux Para Todos. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en [castellano](#). La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

Introducción.

La interconectividad entre un equipo con GNU/Linux® instalado y el resto de los equipos en red en una oficina con alguna versión de Windows® es importante, ya que esto nos permitirá compartir archivos e impresoras. Esta interconectividad se consigue exitosamente a través de [SAMBA](#).

[SAMBA](#) es un conjunto de programas, originalmente creados por Andrew Tridgell y actualmente mantenidos por [The SAMBA Team](#), bajo la Licencia Pública General [GNU](#), y que implementan en sistemas basados sobre UNIX® el protocolo **Server Message Block** (o protocolo **SMB**). Este es algunas veces referido también como **Common Internet File System** ([CIFS](#)), LanManager o protocolo NetBIOS. Sirve como reemplazo total para Windows® NT, Warp®, NFS® o servidores Netware®.

Software requerido.

Los procedimientos descritos en este manual han sido probados para poder aplicarse en sistemas con Red Hat™ Enterprise Linux 3.0, o equivalentes o versiones superiores, y al menos Samba 3.0.7 o versiones superiores.

Necesitará tener instalados los siguientes paquetes, que **seguramente vienen incluidos** en los CD de instalación de su distribución predilecta:

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

Pregunte al sistema si se encuentran instalados estos paquetes, utilizando el siguiente mandato:

```
rpm -q samba samba-client samba-common
```

Si se utiliza Red Hat™ Enterprise Linux, solo bastará ejecutar lo siguiente para instalar o actualizar el software necesario:

```
up2date -i samba samba-client
```

Si utiliza White Box Enterprise Linux u otros clones de Red Hat™ Enterprise Linux o bien sistemas que utilicen yum, solo bastará ejecutar lo siguiente para instalar o actualizar el software necesario:

```
yum -y install samba samba-client
```

Configuración básica de Samba.

Para la mayoría de los casos la configuración de Samba como servidor de archivos es suficiente.

Alta de cuentas de usuario.

Es importante sincronizar las cuentas entre el servidor Samba y las estaciones Windows®. Es decir, si en una máquina con Windows® ingresamos como el usuario *"paco"* con clave de acceso *"elpatito16"*, en el servidor Samba deberá existir también dicha cuenta con ese mismo nombre y la misma clave de acceso. Como la mayoría de las cuentas de usuario que se utilizarán para acceder hacia samba no requieren acceso al interprete de mandatos del sistema, no es necesario asignar clave de acceso con el mandato **passwd** y se deberá definir **/sbin/nologin** o bien **/bin/false** como interprete de mandatos para la cuenta de usuario involucrada.

```
useradd -s /sbin/nologin usuario-windows  
smbpasswd -a usuario-windows
```

No hace falta se asigne una clave de acceso en el sistema con el mandato **passwd** puesto que la cuenta no tendrá acceso al interprete de mandatos.

Si se necesita que las cuentas se puedan utilizar para acceder hacia otros servicios como serían Telnet, SSH, etc, es decir, que se permita acceso al interprete de mandatos, será necesario especificar / **bin/bash** como interprete de mandatos y además se deberá asignar una clave de acceso en el sistema con el mandato **passwd**:

```
useradd -s /bin/bash usuario-windows
passwd usuario-windows
smbpasswd -a usuario-windows
```

El fichero lmhosts

Es necesario empezar resolviendo localmente los nombres NetBIOS asociándolos con direcciones IP correspondientes. Para fines prácticos el nombre *NetBIOS* debe tener un máximo de 11 caracteres. Normalmente tomaremos como referencia en nombre corto de servidor o el nombre corto que se asigne como alias a la interfaz de red. Este lo estableceremos en el fichero **/etc/samba/lmhosts**, en donde encontraremos lo siguiente:

```
127.0.0.1 localhost
```

Debemos añadir entonces el nombre que hayamos elegido asociado a la dirección IP que se tenga dentro de la red local. **Opcionalmente** podrá añadir también los nombres y dirección IP del resto de las máquinas que conformen la red local. La separación de espacios se hace con un tabulador.

Ejemplo:

```
127.0.0.1 localhost
192.168.1.5 maquinainux
192.168.1.6 isaac
192.168.1.7 finanzas
192.168.1.8 direccion
```

Parámetros principales del fichero smb.conf.

Edite el fichero **/etc/samba/smb.conf** con cualquier editor de texto. Dentro de este notará que la información que le será de utilidad viene comentada con un símbolo **#** y los ejemplos con **;** (punto y coma), siendo estos últimos los que tomaremos como referencia.

Empezaremos por establecer el grupo de trabajo editando el valor del parámetro **workgroup** asignando un grupo de trabajo deseado:

```
workgroup = MIGRUPO
```

Opcionalmente puede establecer con el parámetro **netbios name** otro nombre distinto para el servidor si acaso fuese necesario, pero siempre tomando en cuenta que dicho nombre deberá corresponder con el establecido en el fichero `/etc/samba/lmhosts`:

```
netbios name = maquinaLinux
```

El parámetro **server string** es de carácter descriptivo. Puede utilizarse un comentario breve que de una descripción del servidor.

```
server string = Servidor Samba %v en %L
```

Parámetros útiles para la seguridad.

La seguridad es importante y esta se puede establecer primeramente estableciendo la lista de control de acceso que definirá que máquinas o redes podrán acceder hacia el servidor. El parámetro **hosts allow** sirve para determinar esto. Si la red consiste en la máquinas con dirección IP desde 192.168.1.1 hasta 192.168.1.254, el rango de direcciones IP que se definirá en `hosts allow` será **192.168.1.** de modo tal que solo se permitirá el acceso dichas máquinas. Note por favor el punto al final de cada rango. Edite ésta de manera que quede del siguiente modo:

```
hosts allow = 192.168.1. 127.
```

El parámetro **interfaces** permite establecer desde que interfaces de red del sistema se escucharán peticiones. Samba no responderá a peticiones provenientes desde cualquier interfaz no especificada. Esto es útil cuando Samba se ejecuta en un servidor que sirve también de puerta de enlace para la red local, impidiendo se establezcan conexiones desde fuera de la red local.

```
interfaces = 192.168.1.254/24
```

Impresoras en Samba.

Las impresoras se comparten de modo predeterminado, así que solo hay que realizar algunos ajustes. Si se desea que se pueda acceder hacia la impresora como usuario invitado sin clave de acceso, basta con añadir **public = Yes** en la sección de impresoras del siguiente modo:

```
[printers]
comment = El comentario que guste.
path = /var/spool/samba
printable = Yes
browseable = No
public = Yes
```

Windows NT, 2000 y XP no tendrán problema alguno para acceder e imprimir hacia las impresoras, sin embargo Windows 95, 98 y ME suelen tener problemas para comunicarse con Samba para poder imprimir. Por tanto, si se quiere evitar problemas de conectividad con dichos sistemas operativos hay que agregar algunos parámetros que resolverán cualquier eventualidad:

```
[printers]
comment = Impresoras.
path = /var/spool/samba
printable = Yes
browseable = No
public = Yes
print command = lpr -P %p -o raw %s -r
lpq command = lpstat -o %p
lprm command = cancel %p-%j
```

Se puede definir también a un usuario o bien un grupo (**@grupo_que_sea**) para la administración de las colas de las impresoras:

```
[printers]
comment = Impresoras.
path = /var/spool/samba
printable = Yes
browseable = No
public = Yes
print command = lpr -P %p -o raw %s -r
lpq command = lpstat -o %p
lprm command = cancel %p-%j
printer admin = fulano, @opers_impresion
```

Con lo anterior se define que el usuario **fulano** y quien pertenezca al grupo **opers_impresion** podrán realizar tareas de administración en las impresoras.

Compartiendo directorios a través de Samba.

Para los directorios o volúmenes que se irán a compartir, en el mismo fichero de configuración encontrará distintos ejemplos para distintas situaciones particulares. En general, puede utilizar el siguiente ejemplo que funcionará para la mayoría:

```
[Lo_que_quiera]
comment = Comentario que se le ocurra
path = /cualquier/ruta/que/desea/compartir
```

El volumen puede utilizar cualquiera de las siguientes opciones:

Opción	Descripción
guest ok	Define si se permitirá el acceso como usuario invitado. El valor puede ser Yes o No.
public	Es un equivalente del parámetro guest ok , es decir define si se permitirá el acceso como usuario invitado. El valor puede ser Yes o No.
browseable	Define si se permitirá mostrar este recurso en las listas de recursos compartidos. El valor puede ser Yes o No.
writable	Define si se permitirá la escritura. Es el parámetro contrario de read only. El valor puede ser Yes o No. Ejemplos: «writable = Yes» es lo mismo que «read only = No». Obviamente «writable = No» es lo mismo que «read only = Yes»
valid users	Define que usuarios o grupos pueden acceder. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo precedidos por una @. Ejemplo: fulano, mengano, @administradores
write list	Define que usuarios o grupos pueden acceder con permiso de escritura. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo precedidos por una @. Ejemplo: fulano, mengano, @administradores
admin users	Define que usuarios o grupos pueden acceder con permisos administrativos para el recurso. Es decir, podrán acceder hacia el recurso realizando todas las operaciones como super-usuarios. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo precedidos por una @. Ejemplo: fulano, mengano, @administradores
directory mask	Es lo mismo que directory mode. Define que permiso en el sistema que tendrán los subdirectorios creados dentro del recurso. Ejemplos: 1777

<code>create mask</code>	Define que permiso en el sistema que tendrán los nuevos ficheros creados dentro del recurso. Ejemplo: 0644
--------------------------	--

En el siguiente ejemplo se compartirá a través de Samba el recurso denominado «ftp», el cual está localizado en el directorio `/var/ftp/pub` del disco duro. Se permitirá el acceso a cualquiera pero será un recurso de solo lectura salvo para los usuarios administrador y fulano. Todo directorio nuevo que sea creado en su interior tendrá permiso 755 y todo fichero que sea puesto en su interior tendrá permiso 644.

```
[ftp]
comment = Directorio del servidor FTP
path = /var/ftp/pub
guest ok = Yes
read only = Yes
write list = fulano, administrador
directory mask = 0755
create mask = 0644
```

Configuración avanzada de Samba.

Samba fue creado con un objetivo: ser en un reemplazo definitivo para Windows como servidor en una red local. Ésto, por supuesto, requiere algunos procedimientos adicionales dependiendo de las necesidades de la red local.

Re-asignación de grupos de Windows en Samba.

Los grupos que existen en Windows también se utilizan en Samba para ciertas operaciones, principalmente relacionadas con lo que involucra un Controlador Primario de dominio (o **PDC** que significa **P**rimary **D**omain **C**ontroler). Estos grupos existen de modo predefinido en Samba. Sin embargo, si se ejecuta lo siguiente:

```
net groupmap list
```

Devolverá la siguiente información:

```
System Operators (S-1-5-32-549) -> -1
Domain Admins (S-1-5-21-XXXXXXXXXXXX-XXXXXXXXXXXX-XXXXXXXXXXXX-512) -> -1
Replicators (S-1-5-32-552) -> -1
Guests (S-1-5-32-546) -> -1
Domain Guests (S-1-5-21-XXXXXXXXXXXX-XXXXXXXXXXXX-XXXXXXXXXXXX-514) -> -1
Power Users (S-1-5-32-547) -> -1
Print Operators (S-1-5-32-550) -> -1
Administrators (S-1-5-32-544) -> -1
Account Operators (S-1-5-32-548) -> -1
Domain Users (S-1-5-21-XXXXXXXXXXXX-XXXXXXXXXXXX-XXXXXXXXXXXX-513) -> -1
Backup Operators (S-1-5-32-551) -> -1
Users (S-1-5-32-545) -> -1
```

Lo anterior corresponde al mapa de los grupos que, de modo predeterminado, utilizará Samba si éste fuese configurado como Controlador Primario de Dominio. **XXXXXXXXXXXX-XXXXXXXXXXXX-XXXXXXXXXXXX** corresponde a un número generado aleatoriamente al iniciarse Samba por primera vez. **Tome nota de dicho número, ya que lo requerirá más adelante** para re-asignar los nombres al español en el mapa de grupos.

Los grupos anteriormente descritos **trabajarán perfecta y limpiamente** asociándolos contra grupos en el sistema, pero **solo si utiliza alguna versión de Windows en ingles**. Si utiliza alguna versión de Windows en español, **habrá que re-asignar los nombres de los grupos a los correspondientes al español** y asociarles a grupos en el sistema, esto a fin de permitir asignar usuarios a dichos grupos y de este modo delegar tareas de administración del mismo modo que en Windows.

Es por tal motivo que si se tiene la intención de configurar Samba como Controlador Primario de Dominio y al mismo tiempo poder hacer uso de los grupos del mismo modo que en Windows, es decir, por mencionar un ejemplo, permitir a ciertos usuarios pertenecer al grupo de administradores del dominio con privilegios de administrador, lo primero será entonces generar los grupos en el sistema ejecutando como root los siguientes mandatos:

```

groupadd -r administradores
groupadd -r admins_dominio
groupadd -r duplicadores
groupadd -r invitados
groupadd -r invs_dominio
groupadd -r opers_copias
groupadd -r opers_cuentas
groupadd -r opers_impresion
groupadd -r opers_sistema
groupadd -r usrs_avanzados
groupadd -r usuarios
groupadd -r usuarios_dominio

```

Una vez creados los grupos en el sistema, solo resta re-asignar los nombres al español en el mapa de grupo de Samba y asociarles a éstos los grupos recién creados en el sistema. El procedimiento se resume a ejecutar algo como lo siguiente:

```

net groupmap modify \
ntgroup="Nombre grupo Windows en español" \
sid="número-de-identidad-en-sistema \
unixgroup=grupo_en_linux \
comment="comentario descriptivo acerca del grupo"

```

Lo anterior establece que se modifique el registro del grupo que corresponda al **sid** (identidad de sistema) definido con el nombre establecido con **ntgroup**, asociándolo al grupo en el servidor con **unixgroup** y añadiendo un comentario descriptivo acerca de dicho grupo con **comment**.

De modo tal, y a fin de facilitar las cosas a quien haga uso de este manual, puede utilizar el siguiente guión para convertir los nombres al español y asociarlos a grupos en Linux, donde solo deberá definir el número de identidad del sistema que corresponda al servidor:

```

#!/bin/sh
SIDSAMBA=XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX

net groupmap modify ntgroup="Administradores" \
sid="S-1-5-32-544" unixgroup=administradores \
comment="Los administradores tienen acceso completo y sin restricciones al equipo o dominio"

net groupmap modify ntgroup="Admins. del dominio" \
sid="S-1-5-21-$$SIDSAMBA-512" unixgroup=admins_dominio \
comment="Administradores designados del dominio"

net groupmap modify ntgroup="Duplicadores" \
sid="S-1-5-32-552" unixgroup=duplicadores \
comment="Pueden duplicar archivos en un dominio"

net groupmap modify ntgroup="Invitados del dominio" \
sid="S-1-5-21-$$SIDSAMBA-514" unixgroup=invitados \
comment="Todos los invitados del dominio"

```

```

net groupmap modify ntgroup="Invitados" \
sid="S-1-5-32-546" unixgroup=invitados \
comment="Los invitados tienen de modopredeterminado el mismo acceso que los
miembros del grupo Usuarios, excepto la cuenta Invitado que tiene mas
restricciones"

net groupmap modify ntgroup="Operadores de copias" \
sid="S-1-5-32-551" unixgroup=opers_copias \
comment="Los operadores de copia pueden sobrescribir restricciones de seguridad
con el unico proposito de hacer copias de seguridad o restaurar archivos"

net groupmap modify ntgroup="Oper. de cuentas" \
sid="S-1-5-32-548" unixgroup=opers_cuentas \
comment="Pueden administrar cuentas de usuarios y grupos del dominio"

net groupmap modify ntgroup="Oper. de impresión" \
sid="S-1-5-32-550" unixgroup=opers_impresion \
comment="Pueden operar impresoras del dominio"

net groupmap modify ntgroup="Oper. de servidores" \
sid="S-1-5-32-549" unixgroup=opers_sistema \
comment="Pueden administrar sistemas del dominio"

net groupmap modify ntgroup="Usuarios avanzados" \
sid="S-1-5-32-547" unixgroup=usrs_avanzados \
comment="Los usuarios avanzados tienen mas derechos administrativos con algunas
restricciones. De este modo, pueden ejecutar aplicaciones heredadas junto con
aplicaciones certificadas"

net groupmap modify ntgroup="Usuarios del dominio" \
sid="S-1-5-21- $\$$ SIDSAMBA-513" unixgroup=usuarios_dominio \
comment="Todos los usuarios del dominio"

net groupmap modify ntgroup="Usuarios" \
sid="S-1-5-32-545" unixgroup=usuarios \
comment="Los usuarios no pueden hacer cambios accidentales o intencionados en
el sistema. Pueden ejecutar aplic. certificadas, pero no la mayoría de las
heredadas"

exit 0

```

Nota: Este guión en esta incluido en el disco de “Extras de curso” de Linux Para Todos. Solo basta editarlo y definir la variable SIDSAMBA y ejecutarlo como root.

Una vez hecho lo anterior, al volver a ejecutar lo siguiente:

```
net groupmap list
```

Se deberá de mostrar ahora esto otro:

```
Opers. de servidores (S-1-5-32-549) -> opers_sistema
Admins. del dominio (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-
XXXXXXXXXX-512) -> admins_dominio
Duplicadores (S-1-5-32-552) -> duplicadores
Invitados (S-1-5-32-546) -> invitados
Invitados del dominio (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-
XXXXXXXXXX-514) -> invitados
Usuarios avanzados (S-1-5-32-547) -> usrs_avanzados
Opers. de impresión (S-1-5-32-550) -> opers_impresion
Administradores (S-1-5-32-544) -> administradores
Opers. de cuentas (S-1-5-32-548) -> opers_cuentas
Usuarios del dominio (S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-
XXXXXXXXXX-513) -> usuarios_dominio
Operadores de copias (S-1-5-32-551) -> opers_copias
Usuarios (S-1-5-32-545) -> usuarios
```

De este modo, si por ejemplo, se agrega al usuario fulano al grupo **admins_dominio**, se tendrá el mismo efecto que si se hiciera lo mismo en Windows agregando al usuario al grupo **Admins. del dominio**. Esto por supuesto solamente tendrá utilidad si Samba se configura y utiliza como Controlador Primario de Dominio.

Alta de cuentas de usuario en Controlador Primario de Dominio.

Si se configuró Samba para funcionar como Controlador Primario de Dominio, será necesario asignar a root una clave de acceso en Samba, la cual por supuesto puede ser diferente a la del sistema, debido a que las estaciones de trabajo necesitan autenticar primero con el usuario root de Samba para poder unirse dominio y poder crear de este modo una cuenta de máquina en el sistema a través del parámetro **add machine script** ya descrito anteriormente.

Los usuarios es necesario darlos de alta de modo que queden agregados a los que correspondan en el sistema a grupos **Usuarios** y **Usuarios del dominio** de Windows, es decir a los grupos **usuarios** y **usuarios_dominio**.

```
useradd -s /sbin/nologin -G usuarios,usuarios_dominio
usuario-windows
smbpasswd -a usuario-windows
```

Si el usuario ya existiese, solo será necesario agragarlo a los grupos **usuarios** y **usuarios_dominio** con **gpasswd** del siguiente modo:

```
gpasswd -a usuario-windows usuarios
gpasswd -a usuario-windows usuarios_dominio
```

En teoría en el directorio definido para el recurso **Profiles** se deben crear automáticamente los directorios de los usuarios donde se almacenarán los perfiles. De ser necesario es posible generar éstos directorios utilizando el siguiente guión:

```
cd /home
for user in *
do
mkdir -p /var/lib/samba/profiles/$user
chown $user.$user /var/lib/samba/profiles/$user
done
```

Parámetros de configuración avanzada en el fichero smb.conf

Anunciando el servidor Samba en los grupos de trabajo.

La opción **remote announce** se encarga de que el daemon nmbd se anuncie a si mismo de forma periódica hacia una red en particular y un grupo de trabajo específico. Esto es particularmente útil si se necesita que el servidor Samba aparezca no solo en el grupo de trabajo al que pertenece sino también otros grupos de trabajo. El grupo de trabajo de destino puede estar en donde sea mientras exista una ruta y sea posible la transmisión exitosa de paquetes.

```
remote announce = 192.168.1.255/MI-DOMINIO 192.168.2.255/
OTRO-DOMINIO
```

El ejemplo anterior definió que el servidor Samba se anuncie a si mismo al los grupos de trabajo MI-DOMINIO y OTRO-DOMINIO en las redes cuyas IP de transmisión son 192.168.1.255 y 192.168.2.255 correspondientemente.

Ocultando y denegando acceso a ficheros.

No es conveniente que los usuarios acceder o bien puedan ver la presencia de ficheros ocultos en el sistema, es decir ficheros cuyo nombre comienza con un punto, particularmente si acceden a su directorio personal en el servidor Samba (.bashrc, .bash_profile, .bash_history, etc.). Puede utilizarse el parámetro **hide dot files** para mantenerlos ocultos.

```
hide dot files = Yes
```

En algunos casos puede ser necesario denegar el acceso a cierto tipo de ficheros del sistema. El parámetro **veto files** se utiliza para especificar la lista, separada por diagonales, de aquellas cadenas de texto que denegarán el acceso a los ficheros cuyos nombres contengan estas cadenas. En el siguiente ejemplo, se denegará el acceso hacia los ficheros cuyos nombres incluyan la palabra «Security» y los que tengan extensión o terminen en «.tmp»:

```
veto files = /*Security*//*.tmp/
```

Opciones para cliente o servidor Wins

Puede habilitar convertirse en servidor WINS o bien utilizar un servidor WINS ya existente. Se puede ser un servidor WINS o un cliente WINS, pero no ambas cosas a la vez.

Si se va a ser el servidor WINS, debe habilitarse lo siguiente:

```
wins support = Yes
```

Si se va a utilizar un servidor WINS ya existente, debe descomentar la siguiente línea y especificar que dirección IP utiliza dicho servidor WINS:

```
wins server = 192.168.1.1
```

Opciones específicas para Controlador Primario de Dominio (PDC).

Si se va a configurar Samba como Controlador Primario de Dominio, se debe especificar todos los parámetros descritos a continuación.

Si se quiere que las claves de acceso del sistema y Windows se mantengan sincronizadas, es necesario descomentar las siguientes líneas:

```
unix password sync = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *New*UNIX*password* %n\n
*ReType*new*UNIX*password* %n\n
*passwd:*all*authentication*tokens*updated*successfully*
```

El parámetro **local master** define al servidor como examinador del dominio (o master browser); El parámetro **domain master** define al servidor maestro del dominio; El parámetro **preferred master** define al servidor como maestro del dominio preferido en caso de haber más servidores presentes en el mismo dominio como controladores de dominio; El parámetro **time server** se utiliza para definir que las estaciones deberán sincronizar la hora con el servidor al unirse al dominio; El parámetro **domain logons** define que el servidor permitirá a las estaciones autenticar contra Samba.

```
local master = Yes
domain master = Yes
preferred master = Yes
time server = Yes
domain logons = Yes
```

La configuración de Controlador Primario de Dominio requiere además definir donde se almacenarán los perfiles de los usuarios. Windows 95, 98 y ME requieren se defina con el parámetro **logon home**, en tanto que Windows NT, 2000 y XP requieren se haga con el parámetro **logon path**. Para efectos prácticos y de previsión, utilice ambos parámetros y defina la unidad H para dicho volumen:

```
logon path = \\%L\Profiles\%U
logon home = \\%L\%U\.profile
logon drive = H:
```

Si se va a utilizar Samba como Controlador Primario de Dominio, es necesario establecer el guión que ejecutarán las estaciones Windows al conectarse hacia el servidor. Esto se hace a través del parámetro **logon script** el cual puede definir o bien un guión a utilizar por cada usuario (%u.bat) o bien por cada máquina (%m.bat) o bien de modo general para todos (logon.cmd). Para no complicar las cosas, defina inicialmente un guión general para todos del siguiente modo:

```
logon script = logon.cmd
```

El fichero **/var/lib/samba/netlogon/logon.cmd** deberá contener algo como lo siguiente:

```
REM windows client logon script
REM

net time \\mi-servidor /SET /YES
net use H: \\mi-servidor\homes /PERSISTENT:NO
```

El Controlador Primario de Dominio va a necesitar también se definan los guiones a ejecutar para distintas tareas como alta de máquinas, usuarios y grupos así como la baja de estos.

```
add user script = /usr/sbin/useradd %u
add machine script = /usr/sbin/useradd -d /dev/null -g
100 -s /bin/false -c "Cuenta de máquina" -M %u
delete user script = /usr/sbin/userdel %u
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/bin/gpasswd -a %u %g
set primary group script = /usr/sbin/usermod -g %g %u
```

El parámetro **add user script** sirve para definir lo que se deberá ejecutar en el trasfondo en el sistema para crear una nueva cuenta de usuario. El parámetro **add machine script** es particularmente importante porque es el mandato utilizado para **dar de alta cuentas de máquinas** (trust accounts o cuentas de confianza) **de modo automático**. El parámetro **delete user script** es para definir lo propio para eliminar usuarios, **delete group script** para eliminar grupos, **add user to group** para añadir usuarios a grupos y set **primary group script** para establecer un grupo como el principal para un usuario.

Directorio para Netlogon y perfiles en Controlador Primario de Dominio (PDC).

Si se va a utilizar Samba como Controlador Primario de Dominio, es necesario definir los recursos donde residirá netlogon y también donde se almacenarán los perfiles de los usuarios:

```
[netlogon]
comment = Network Logon Service
path = /var/lib/samba/netlogon
write list = @administradores, @admins_dominio
guest ok = Yes
browseable = Yes

[Profiles]
path = /var/lib/samba/profiles
read only = No
guest ok = Yes
create mask = 0600
directory mask = 0700
```

Genere con el mandato `mkdir` los directorios `/var/lib/samba/profiles` y `/var/lib/samba/netlogon`. El directorio `/var/lib/samba/profiles` deberá pertenecer a `root` y al grupo `users` y tener permiso `1777` a fin de permitir crear el directorio de perfil correspondiente para cada usuario.

```
mkdir -p -m 1777 /var/lib/samba/profiles
mkdir -p /var/lib/samba/netlogon
chgrp users /var/lib/samba/profiles
```

Inciar el servicio y añadirlo al arranque del sistema.

Si iniciará Samba por primera vez ejecute lo siguiente:

```
/sbin/service smb start
```

Si va a reiniciar el servicio, ejecute lo siguiente:

```
/sbin/service smb restart
```

Para que Samba inicie automáticamente cada vez que inicie el servidor solo ejecute el siguiente mandato:

```
/sbin/chkconfig smb on
```

Accediendo hacia Samba.

Modo texto.

Smbclient.

Indudablemente el método más práctico y seguro es el mandato *smbclient*. Este permite acceder hacia cualquier servidor Samba o Windows® como si fuese el mandato ftp en modo texto.

Para acceder al cualquier recurso de alguna máquina Windows® o servidor SAMBA determine primero que volúmenes o recursos compartidos posee está. utilice el mandato *smbclient* del siguiente modo:

```
smbclient -U usuario -L alguna_maquina
```

Lo cual le devolvería más menos lo siguiente:

```
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.0.7-1.3E]

  Sharename      Type      Comment
  -----
  homes          Disk     Home Directories
  netlogon       Disk     Network Logon Service
  ftp            Disk     ftp
  IPC$           IPC      IPC Service (Servidor Samba 3.0.7-1.3E en mi-servidor)
  ADMIN$         IPC      IPC Service (Servidor Samba 3.0.7-1.3E en mi-servidor)
  ep15900        Printer  Created by redhat-config-printer 0.6.x
  hp2550bw       Printer  Created by redhat-config-printer 0.6.x
Anonymous login successful
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.0.7-1.3E]

  Server          Comment
  -----
  mi-servidor     Servidor Samba 3.0.7-1.3E en mi-servidor

  Workgroup       Master
  -----
  MI-DOMINIO     MI-SERVIDOR
```

La siguiente corresponde a la sintaxis básica para poder navegar los recursos compartidos por la máquina Windows® o el servidor SAMBA:

```
smbclient //alguna_maquina/recurso -U usuario
```

Ejemplo:

```
smbclient //LINUX/FTP -U jbarrios
```

Después de ejecutar lo anterior, el sistema solicitará se proporcione la clave de acceso del usuario *jbarrios* en el equipo denominado *LINUX*.

```
smbclient //LINUX/FTP -U jbarrios
added interface ip=192.168.1.254 bcast=192.168.1.255
nmask=255.255.255.0
Password:
Domain=[miusuario] OS=[Unix] Server=[Samba 2.2.1a]
smb: \>
```

Pueden utilizarse virtualmente los mismos mandatos que en el interprete de *ftp*, como serían *get*, *mget*, *put*, *del*, etc.

Por montaje de unidades de red.

Si necesita poder visualizar desde GNU/Linux a las máquinas con Windows® e interactuar con los directorios compartidos por éstas, necesitará realizar algunos pasos adicionales. De manera predeterminada, y por motivos de seguridad, solo *root* puede utilizar los mandatos *smbmnt* y *smbumount*. Deberá entonces establecer permisos de SUID a dichos mandatos. Puede hacerlo ejecutando, como *root* lo siguiente:

```
chmod 4755 /usr/bin/smbmnt
chmod 4755 /usr/bin/sbumount
```

Para acceder hacia una máquina Windows® determine primero que volúmenes o recursos compartidos posee está. utilice el mandato *smbclient* del siguiente modo:

```
smbclient -N -L alguna_maquina
```

Lo cual le devolvería más menos lo siguiente:

```

Anonymous login successful
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.0.7-1.3E]

    Sharename      Type      Comment
    -----
homes             Disk      Home Directories
netlogon          Disk      Network Logon Service
ftp               Disk      ftp
IPC$              IPC       IPC Service (Servidor Samba 3.0.7-1.3E en mi-servidor)
ADMIN$            IPC       IPC Service (Servidor Samba 3.0.7-1.3E en mi-servidor)
ep15900           Printer   Created by redhat-config-printer 0.6.x
hp2550bw          Printer   Created by redhat-config-printer 0.6.x
Anonymous login successful
Domain=[MI-DOMINIO] OS=[Unix] Server=[Samba 3.0.7-1.3E]

    Server          Comment
    -----
mi-servidor        Servidor Samba 3.0.7-1.3E en mi-servidor

Workgroup          Master
-----
MI-DOMINIO        MI-SERVIDOR

```

En el ejemplo anterior hay un volumen compartido llamado *algún_volumen*. Si queremos montar este, debemos crear un punto de montaje. Éste puede crearse en cualquier directorio sobre el que tengamos permisos de escritura. Para montarlo, utilizamos entonces la siguiente línea de mandato:

```
smbmount //alguna_maquina/algún_volumen /punto/de/montaje/
```

Si la máquina Windows® requiere un usuario y una clave de acceso, puede añadir a lo anterior las opciones *-username=el_necesario -password=el_requerido -workgroup=MIGRUPO*

Si la distribución de GNU/Linux utilizada es reciente, también puede utilizar el ya conocido mandato *mount* del siguiente modo:

```
mount -t smbfs -o username=el_necesario,
password=el_requerido //alguna_maquina/algún_volumen /
punto/de/montaje/
```

Si se genera una cuenta *pcguest*, similar a la cuenta *nobody*, podemos montar volúmenes SMB sin ingresar una clave de acceso pero con privilegios restringidos, o aquellos que definamos a un volumen accedido por un usuario invitado. Esto sería el método por elección para compartir volúmenes en una red de área local. Puede generarse una cuenta *pcguest* o bien dejar que el sistema tome al usuario *nobody*. Si opta por lo primero, solo de de alta la cuenta **NO** asigne clave de acceso alguna. Montar volúmenes remotos como usuarios invitado es muy sencillo. Un ejemplo real sería:

```
mount -t smbfs -o guest //LINUX/FTP //var/ftp
```

Lo anterior monta un volumen SAMBA de una máquina con GNU/Linux en otra máquina con GNU/Linux.

Puede añadirse también una entrada en */etc/fstab* de modo que sólo tenga que ser tecleado *mount / punto/de/montaje*. Esta línea sería de modo similar al siguiente:

```
//LINUX/FTP /var/ftp smbfs user,auto,guest,ro,gid=100 0  
0
```

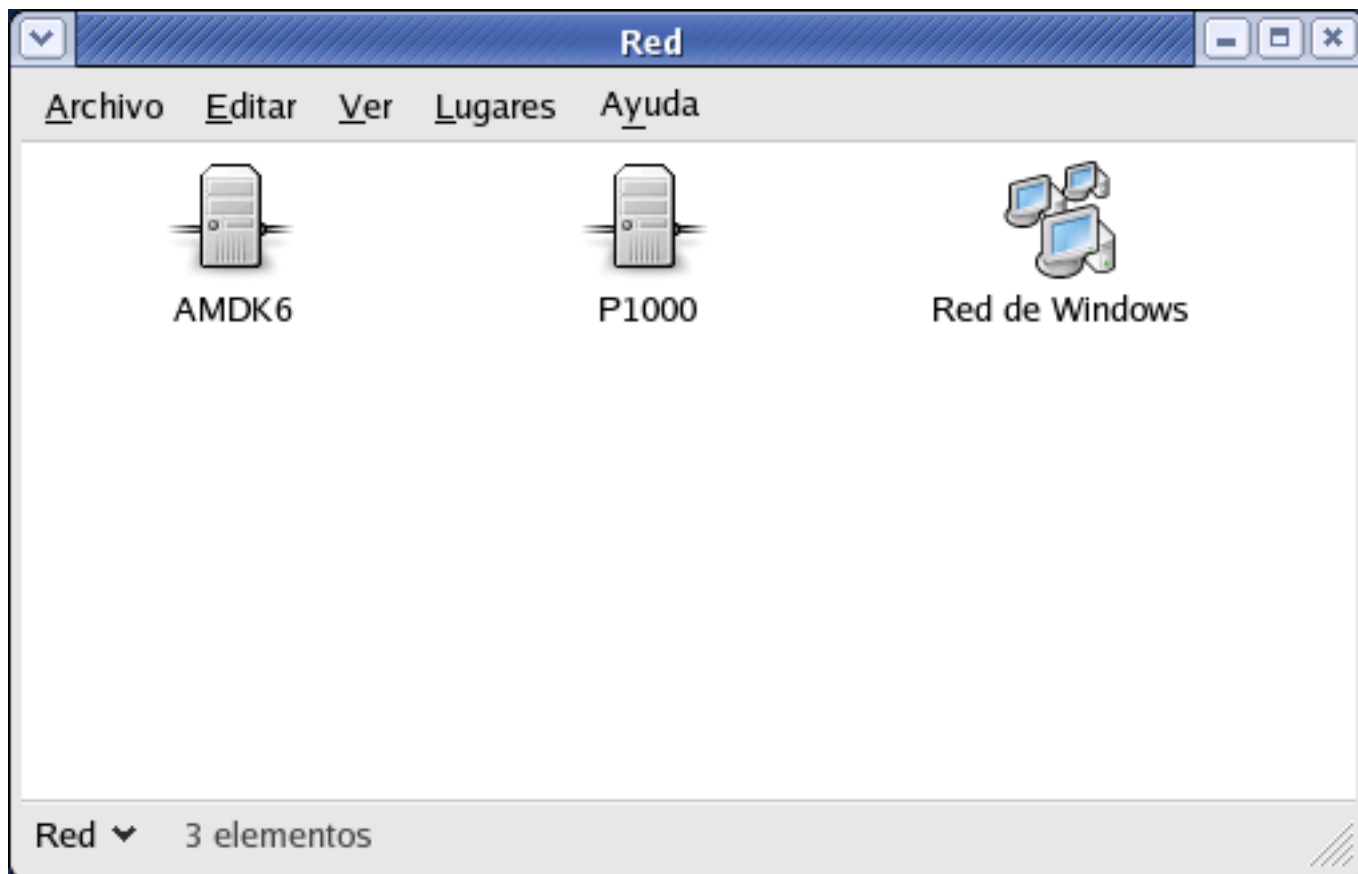
Recuérdese que el volumen compartido debe estar configurado para permitir usuarios invitados:

```
[FTP]  
comment = Software libre (RPMS)  
path = /var/ftp/pub  
public = Yes  
guest ok = Yes
```

Modo gráfico

Desde el entorno de GNOME.

Si utiliza GNOME 2.x o superior, éste incluye un módulo para Nautilus que permite acceder hacia los recursos compartidos a través de Samba sin necesidad de modificar cosa alguna en el sistema. Solo hay que hacer clic en **Servidores de red** en el menú de GNOME.



Desde Windows.

Por su parte, desde Windows deberá ser posible acceder sin problemas hacia Samba como si fuese hacia cualquier otra máquina con Windows. Vaya, ni Windows ni el usuario notarán siquiera la diferencia.

Uniendo máquinas al dominio del Controlador Primario de Dominio.

El controlador de dominio permite utilizar a Samba como servidor de autenticación y servidor de archivos que además permite almacenar el perfil, preferencias y documentos del usuario en el servidor automáticamente sin la intervención del usuario.

Creando manualmente cuentas de máquinas

Bajo algunas circunstancias será necesario crear cuentas de máquinas (trust accounts o cuentas de confianza) a fin de permitir unirse al dominio. el procedimiento es simple:

```
/usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -c  
"Cuenta de máquina" -M maquina-windows$  
smbpasswd -a maquina-windows$
```

Es de resaltar que las cuentas de máquinas deben incluir **obligatoriamente** un símbolo \$ al final del nombre.

Windows 95/98/ME y Windows XP Home

Ya que los sistemas con Windows 95/98/ME y Windows XP Home no incluyen una implementación completa como miembros de dominio, no se requieren cuentas de confianza. El procedimiento para unirse al dominio es el siguiente:

1. Acceder hacia Menú de inicio → Configuraciones → Panel de control → Red
2. Seleccione la pestaña de Configuración
3. Seleccione «Cliente de redes Microsoft»
4. Haga clic en el botón de propiedades
5. Seleccione Acceder a dominio de Windows NT y especifique el dominio correspondiente.
6. Clic en todos los botones de «Aceptar» y reinicie el sistema
7. Acceda con cualquier usuario que haya sido dado de alta en el servidor Samba y que además cuente con una clave de acceso asignada con smbpasswd.

Windows NT

1. Crear manualmente la cuenta de máquina como se describió anteriormente.
2. Acceder hacia Menú de inicio → Configuraciones → Panel de control → Red.
3. Seleccionar la pestaña de «Identificación».
4. Clic en el botón de «Cambiar».
5. Ingrese el nombre del dominio y el nombre del sistema. **No seleccione** «Crear una cuenta de máquina en el Dominio».
6. Clic en «Aceptar»
7. Espere algunos segundos.
8. Deberá mostrarse un mensaje emergente de confirmación que dice «Bienvenido a MI-DOMINIO»
9. Reinicie el sistema
10. Acceda con cualquier usuario que haya sido dado de alta en el servidor Samba y que además cuente con una clave de acceso asignada con smbpasswd.

Windows 2000/2003 y Windows XP Profesional

1. Clic derecho en el icono de «Mi PC».
2. Seleccionar «Propiedades»
3. Haga clic en la pestaña de «Identificación de red» o «Nombre del sistema».
4. Clic en el botón de «Propiedades».
5. Clic en el botón «Miembro de dominio»
6. Ingrese el nombre del dominio y el nombre de la máquina y haga clic en el botón de «Aceptar»
7. Aparecerá un diálogo que preguntará por una cuenta y clave de acceso con privilegios de administración en el servidor. Especifique la root y la clave de acceso que asignó a la cuenta de root con el mandato smbpasswd (**NO LA CLAVE DE ACCESO DE ROOT EN EL**

SISTEMA).

8. Espere algunos segundos.
 9. Deberá mostrarse un mensaje emergente de confirmación que dice «Bienvenido a MI-DOMINIO»
 10. Reinicie el sistema
 11. Acceda con cualquier usuario que haya sido dado de alta en el servidor Samba y que además cuente con una clave de acceso asignada con smbpasswd.
-

Linux Para Todos

<http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=13-como-samba>