artículo

Cómo montar un servidor Samba PDC en una red de máquinas MS Windows XP

Juanma Ginzo

1 Introducción

Voy a escribir un artículo en el que se trata de hacer que un linux corriendo samba haga de servidor como Controlador Primario de Dominio.
La razón por la que escribo esto estriba en que he tenido varios problemas a la hora de configurarlo, y mi deseo consiste en que no os pase a vosotros lo mismo.
La cuestión no es baladí pues hay que tener configurado nuestro samba no solo con las características habituales para usarlo en una red de windows diferentes (95, 98, 2000 etc) sino que además hay que ``retocar'' varias cosas más.
Este artículo seguirá los siguientes pasos:

1. Configurar unas cuantas opciones por defecto en samba
2. Configurar samba como PDC en el fichero smb.conf
3. Crear las cuentas de confianza de las máquinas que tenemos en la red.
4. Configurar las estaciones de trabajo para que se ``autentiquen'' con el PDC

Empezamos pues

2 Configurar opciones por defecto

Aquí poco vamos a colocar, símplemente vamos a darle un nombre al servidor y al grupo de trabajo, además vamos a crear un recurso ``homes'' para que los usuarios vean su directorio home cuando se conecten .

```
[global]

      netbios name = servidor

      workgroup = grupo

      wins support = yes

    [homes]

      writable = yes

      browseable = no
```

En la primera opción le ponemos nombre netbios al servidor. Si teneis DNS ponedle el mismo nombre que el que figura en el dns, sin la coletilla del dominio DNS.

En la segunda opción le decimos a samba que pertenezca al grupo de trabajo ``grupo''. Este dato es importante que lo tengamos en cuenta, pues a la hora de ajustar los clientes, el dominio se va a llamar ``grupo'', que es el mismo que el etiquetado en workgroup.

La opción wins support = yes es de propina. Que samba haga de soporte wins no perjudica a nadie y a samba no le cuesta nada, además es recomendado para que actúe de PDC.

El recurso homes, no home, no hay que confundirse, es un recurso especial pues si está presente hacemos que los usuarios accedan a su directorio home en el servidor.

Decimos que browseable = no para que no se vean en los Windows dos recursos: homes y la carpeta del usuario apuntando los dos al mismo contenido.

La opción writable = yes es para que se pueda escribir y crear elementos en el recurso, pues samba por defecto hace los recursos no escribibles y, en consecuencia, solo lectura.

3 Configurar Samba como PDC

Para ello debemos:

1. Hacer que sea visualizador maestro local y de dominio en la red.
2. Poner la seguridad a nivel de usuario
3. Soportar las passwords encriptadas
4. La más importante: decirle a samba que él es el PDC
5. Además no estaría de más crear el servicio (recurso más bien) netlogon aunque no es estrictamente necesario.

3.1 Visualizador maestro

Un visualizador maestro de dentro de una red windows sirve para proporcionar información a los demás sobre dos aspectos:

- qué puestos hay en la red windows
- qué recursos ofrecen esos puestos a los demás.

Esta facilidad puede soportarla cualquier windows integrado en la red. No es necesario que sea un server. Para ser visualizador maestro solamente se requiere que le toque al equipo de marras.

Nosotros vamos a hacer que esta visualización le toque a nuestro Samba siempre.

Pare ello debemos añadir las líneas siguientes a la sección [global]:

```
os level = 64

preferred master = yes

domain master = yes

local master = yes
```

Pero ¡cuidado! porque debemos asegurarnos de que no exista ningún otro PDC en la red, y tampoco debe haber en la red ningún visualizador maestro de dominio. Si somos los únicos, no hay problema, pero vigilad de forma concienzuda si hay algún servidor w2000 server, o WNT server o algo peor; en caso de que existan no les dejeis que hagan de visualizadores, porque de lo contrario habrá problemas a la hora de ver qué equipos existen en la red y sus recursos.

La opción os level hace referencia a la información del sistema operativo que ofrece Samba. Me explico: cuanto mayor sea este número más avanzado pensarán los demas windows que es el SO de Samba. Para citar un ejemplo si pusieramos el número 34, los windows pensarán que se trata de un Windows NT. Es decir, que con este número engañamos miserablemente a los puestos sobre la versión (windows) de nuestro SO.

Las opciones prefered, domain y local master hacen referencia de que se prefiera a este servidor como visualizador maestro de dominio, local y master sucesivamente.

3.2 Poner la seguridad a nivel de usuario

Esta parte es fácil.

Samba tiene cuatro niveles de seguridad: recurso, usuario, servidor y domain.

La seguridad a nivel de usuario quiere decir que el usuario cuando se autentica en el cliente solo tiene acceso a lo que se le deje tener. En contraposición a nivel de recurso significa que se tiene acceso al recurso cuando pinchando en este desde windows y una vez iniciada la sesión, se nos pide la clave. Si conocemos la clave (seamos quien seamos) entraremos al recurso, si no la conocemos, no entraremos. A nivel de servidor y a nivel de dominio es lo mismo que a nivel de usuario con la diferencia que cuando iniciamos la sesión quien nos autentica es un servidor (no el samba) o un PDC (tampoco el mismo que samba).

Basta añadir en la sección global esto:

security = user

Y con esto ya está.

3.3 Soportar las passwords encriptadas

Es lo más correcto. Las passwords pueden dar vueltas por la red interna encriptadas o no. Le decimos que encriptadas para que nadie las esnife.

Se escribe esto, simplemente:

encrypt passwords = yes

Pero aprovecho este párrafo para añadir y comentar cómo se crean usuarios samba.

Para crear un usuario debemos crearlo anteriormente como usuario unix y, posteriormente darle una contraseña para samba.

adduser usuario

Nos crea un usuario unix, y

smbpasswd -a usuario

Nos crea un usuario samba, que servirá para que los puestos nos autentiquen contra esta contraseña. Mi

recomendación es que la contraseña que creemos en windows sea la misma que la que tengamos en samba Ã‚Â¿de acuerdo? Así nos quitamos líos de encima.

Luego volveré a repetir lo que voy a decir ahora: debemos crear una cuenta de root en samba para que después agreguemos el cliente al dominio.

smbpasswd -a root

Luego indicamos la contraseña dos veces.

Después de agregar todas las máquinas al dominio ¡borra esa cuenta de root!, elimina esa línea del usuario root que aparecerá en el fichero smbpasswd. Es más, en la opción global ``invalid users = usuarios inválidos'' poner por si las moscas a root y demás usuarios que no pertenezcan exclusivamente al dominio de esa red. Símplemente lo digo porque no nos va a apetecer que alguien ande enredando como root (u otro usuario de sistema) por nuestra querida red.

3.4 La más importante: decirle a samba que él es el PDC

Esta es facilita. En la sección global añadir:

domain logons = yes

Con esto el servidor samba dice a la red que él es el PDC.

3.5 Crear el servicio (recurso más bien) netlogon

Este servicio sirve para ejecutar diversos scripts cuando se conecta un windows al servidor. Los scripts son pequeños programas ``por lotes'' escritos desde windows para ejecutar en windows. Digo que hay que escribirlos en windows por las diferentes formas de entender los retornos de carro de un sistema operativo a otro. Y digo que se ejecuta en windows porque se trata de sencillas instrucciones (p.e. ponte en hora con respecto al servidor o net time \\nombre_netbios_servidor_o_IP /set /yes) que solo entiende MSWindows.

En la sección global se escribe esto:

logon script = netlogon.bat

Y se crea un recurso llamado netlogon:

```
[netlogon]

  path = /home/netlogon

  read only = yes
```

En el path copiamos el fichero netlogon.bat construido por nosotros. Si este fichero no existe, no importa pues samba sigue leyendo su configuración.

De esta forma cuando se conecta alguien, se ejecuta el script netlogon.bat y ejecuta lo que deseemos (o podamos) en el cliente.

Solamente un apunte más. Este recurso NO es estrictamente necesario para que funcione la cosa (el PDC), pero me quiero curar en salud pues en todos los manuales que he visto me colocan esta sección como si fuera indudable su uso.

4 Crear las cuentas de confianza de las máquinas que tenemos en la red.

Aquí empezamos con el cogollo de la cuestión.

Resulta que para crear un dominio windows (es decir grupo de trabajo + PDC) en caso de clientes NT, W2000 y XP pro hay que crear lo que se llama cuentas de confianza de las máquinas.

Esas cuentas de confianza es algo que podríamos definir como ``esta máquina y esta otra están en mis dominios''. No solamente los usuarios se autentican y se tienen en cuenta, sino que también las mismas máquinas han de ser tenidas en cuenta.

Para ello hay que crear usuarios en Linux con el nombre netbios de las clientes seguidos del símbolo de dolar.

Lo explico por pasos.

1. Crearemos un grupo, y para evitar líos, con el mismo nombre que le hemos puesto en el smb.conf en la opción workgroup:

   ```
   groupadd grupo
   ```

2. Hay que crear un usuario Unix con el nombre netbios de la máquina y (ojo con esto) seguido del símbolo dolar, sin shell, sin directorio home e integrado en un grupo. El nombre de la máquina es el que figura en el cliente en Panel de Control -> Sistema - Nombre de equipo. Imaginemos el grupo que se llama grupo y la máquina se llame máquina

   ```
   adduser -g grupo -d /dev/null -s /dev/null
   -c ``cliente XP'' maquina$
   ```

   Si observamos el fichero /etc/password, veremos una entrada que empieza por maquina$ que es la cuenta de la máquina.
3. Hay que crear la cuenta de confianza añadiendo a smbpasswd la máquina:

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

Observa con cuidado que aquí no hace falta poner el símbolo de dólar. Hay que indicar, eso sí, que se trata de una máquina (la opción -m). No va a pedir contraseñas.
Si hay más máquinas, pues lo mismo para cada una de ellas.

Con todo esto ya está hecho el trabajo en lo que respecta al servidor.

5 Configurar las estaciones de trabajo para que se ``autentiquen'' con el PDC

5.1 Preparar el cliente

Esta es la parte más diferenciada con respecto a clientes W2000, WNT y W98/95.

Resulta que WXP home no puede integrarse en un dominio Windows. En cambio el XP profesional sí.

Hay que hacer y comprobar los siguientes pasos:

1. Ir a Panel de Control -> Herramientas Administrativas -> Directivas de Seguridad local y mirar Directivas Locales -> Opciones de seguridad
2. Miembro de dominio: descifrar o firmar digitalmente datos de un canal seguro (siempre): Deshabilitar
3. Miembro de dominio: Deshabilitar cambios password en cuenta máquina -> deshabilitar
4. Miembro de dominio: Requerir clave de sesión protegida (W2000 o más reciente) -> deshabilitar
5. Cambiar una cosilla del registro. Esto merece comentario aparte.
   Hay un archivo en /usr/share/doc/samba.XXXX/docs/Registry/ que se llama WinXP_SignOrSeal.reg. Este archivo lo guardamos en un diskette y en cada cliente le damos dos clicks para que se agregue su información al registro de windows.

   Simplemente cambia esta línea del registro dejándola así:

   ```
   [HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Services\Netlogon\Parameters]

       "requiresignorseal"=dword:00000000
   ```

   Con esto hemos preparado el cliente. Solo falta agregarlo a nuestro dominio.

5.2 Agregar el cliente al dominio.

Vamos a Panel de Control -> Sistema y pinchamos en la pestaña ``Nombre del equipo''

Vereis una descripción del equipo. Pues escribís lo que deseéis.

Pincháis en el botón ``Cambiar''

Nombre del equipo: en nuestro ejemplo maquina.

Miembro de: elegimos dominio.

El nombre del dominio es el nombre ``WorkGroup'' del archivo smb.conf.

Le damos a aceptar y nos pide un usuario y una contraseña.

Esto me dio guerra.

Hay que poner root (sí root) y la contraseña de root del servidor.

Nos dará la bienvenida.

Una cosa: el usuario root tiene que estar agregado en el fichero smbpasswd, para que el cliente pueda autenticarlo y así tenerlo en el dominio, pero agregad root solamente para esta cuestión, luego (una vez configurada toda la red) es recomendable borrarlo, porque Ã‚Â¿no querremos que exista un usuario samba que se llame root?Ã‚Â¿verdad? a partir de allí root no tiene que estar agregado a smbpasswd. No sé si repetirlo más veces ... si: root NO tiene que estar agregado a smbpasswd.

Con todo esto tiene que funcionar.

6 Agradecimientos

A mis alumnos: que me hacen moverme por mundos en los que no deseo moverme y que si no fuera por ellos yo no hubiera instalado un Windows XP ni de broma para probar esto.

A mi esposa: que no se por qué obscura razón no deja de una vez de utilizar Windows.