Active Directory en Linux

DIRECTORIOS INTELIGENTES

Hace mucho, mucho tiempo, en una galaxia muy, muy lejana, el mundo del software libre y el de Microsoft se encontraban aislados. Pertenecías a una red o a la otra, pero no a ambos. Entonces a un pequeño grupo de valientes pensaron que esto podía arreglarse. Así nació Samba.. **POR JOSE MARÍA RUÍZ**

A comienzos de 1992 Andrew Tridgell, un ingeniero informático australiano que se encontraba realizando sus estudios de doctorado, se encontró con un problema. Trabajaba en una máquina UNIX (Linux estaba aún en la mente de Linus Torvalds) y necesitaba montar en una máquina MS-DOS un directorio de su UNIX a través de la red. Lo había hecho hasta entonces usando NFS, pero ahora necesitaba que funcionase sobre NetBIOS.

Se armó de paciencia, programó un filtrador de paquetes y comenzó a realizar pruebas para poder replicar el comportamiento del protocolo de Microsoft. NetBIOS es la base de la tecnología de Microsoft para compartir ficheros a través de red. Cuando consiguió un programa que le permitió realizar esta hazaña lo liberó. Eran los primeros 90 y lo que sería Samba daba sus primeros pasos.

Ese pequeño programa pasó inadvertido, incluso para el propio Andrew, hasta 1994. En ese entonces quiso conectar el equipo con Windows de su mujer al suyo, que ejecutaba Linux. Se acordó del pequeño servidor que programó dos años antes y lo probó. Para su sorpresa ¡funcionaba!

Investigó un poco y descubrió que los protocolos NetBIOS y SMB, que usan las máquinas de Microsoft, estaban documentados aunque se dejaban muchos parámetros sin especificar. Decidió realizar una programa serio, ahora que tenía

la experiencia necesaria. Y, como uno de sus primeros pasos, Andrew buscó nombre para el proyecto. Escogió *smb*, pero entonces se percató de que estaba registrado. Así que ni corto ni perezoso introdujo *smb* en un editor de textos y esperó que el corrector ortográfico decidiese por él. La primera palabra que apareció fue *Samba* y así fue llamado desde entonces.

Samba ha crecido sin parar desde entonces, añadiendo más funcionalidades y batiendo en numerosas ocasiones al propio software de Microsoft en cuanto a seguridad y rendimiento. El nombre del proyecto Samba apareció en los famosos *documentos de Halloween* donde Microsoft se quejaba del daño provocado por los proyectos libres.

Samba cuenta ahora con gran cantidad de programadores voluntarios, tiene una conferencia anual (Samba eXPerience) y el apoyo de grandes empresas como Silicon Graphics, Novell o IBM.

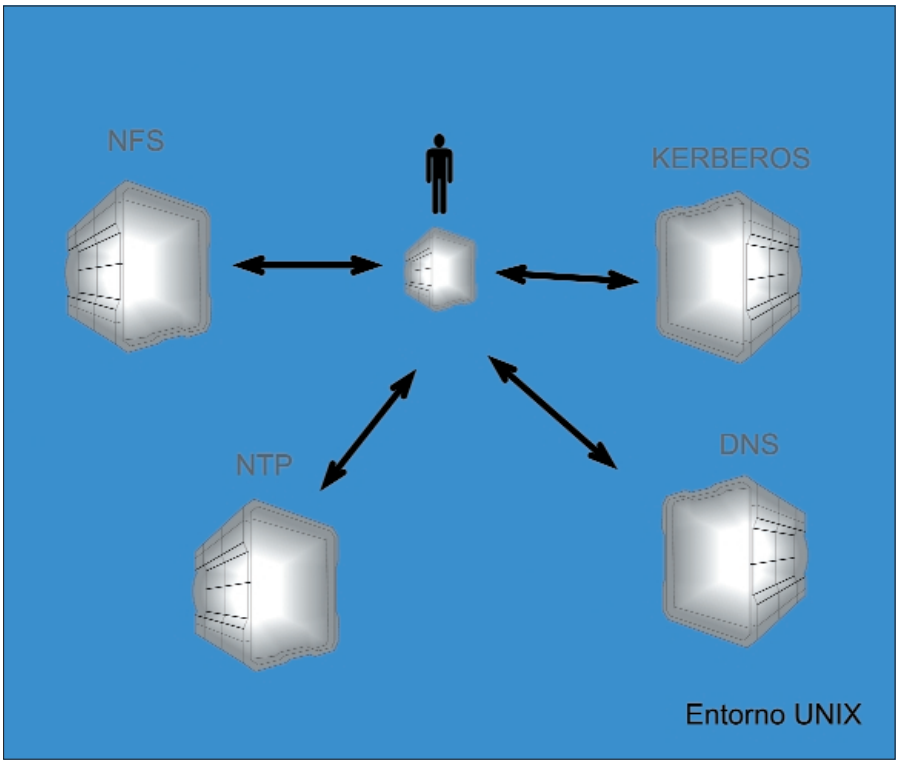

Figura 1: Esquema típico de una red Linux.

La Situación Actual

Samba ha ido amoldándose a la situación a medida que Microsoft añadía funcionalidades o modificaba sus protocolos. En un principio Samba permitía a una máquina Linux compartir directorios con una máquina Windows. Era el famoso *compartir carpeta*.

Posteriormente fue posible montar carpetas compartidas por máquinas Windows como directorios en equipos Linux. De esta manera el acceso a su contenido era como el acceso a un directorio local. También se añadió la posibilidad de usar impresoras remotas o compartir las propias.

Microsoft, ya por aquel entonces, comenzó a explotar el filón empresarial con la versión NT de su sistema operativo. Windows NT incorporaba la posibilidad de gestionar el acceso a las máquinas Windows NT o 95 a través de los *dominios*. La gente de Samba decidió pasar a la acción y trabajó intensamente en la replicación de este servicio.

Sus esfuerzos fueron recompensados y fue posible registrar a una máquina Samba en una máquina NT en esta tarea. Al poco tiempo, entre 1999 y el año 2000, hubo un fork (una escisión) y se creó un proyecto paralelo denominado *Samba TNG*. La misión de este otro proyecto, que comparte gran parte del código de Samba, es realizar un reemplazo total de las características de Windows NT como controlador de dominio. *Samba TNG* ha ido apagándose poco a poco, y aunque persisten algunos de sus colaboradores muchos lo dan por abandonado.

La gente de Samba avanzó por su cuenta, siguiendo otros criterios. En septiembre del 2003 se pudo registrar una máquina Samba en una máquina Active Directory.

Y a finales de 2003, en diciembre, se consiguió replicar completamente un dominio Windows NT, incluyendo la migración de usuarios y claves. Samba estaba entonces en la versión 3.0.x. Samba podía sustituir a un Windows NT Server completamente. Esto supuso un boom, puesto que muchas empresas se interesaron por la tecnología ya que así se ahorraban licencias, bastante caras, de Windows NT Server.

Pero la gran desventaja de Samba es que siempre va unos pasos por detrás de Microsoft. Este seguimiento continuo ha llevado a un código fuente difícil de mantener y de cambiar. Por eso Andrew Tridgell y otros se han lanzado al desarrollo de Samba4: una reescritura parcial de Samba3 buscando la modularidad y el reemplazo total de una máquina Active Directory.

Primeros pasos con Samba

Lo primero que haremos será instalar Samba. La manera de hacerlo dependerá de la distribución que usemos. Puede que tengamos que descargar el paquete o que exista una herramienta que lo instale por nosotros. Hay que asegurarse de instalar tanto el servidor de Samba como las herramientas cliente. Existen

Cuadro 1: smb.conf para configuración local

```
01 [global]
02         workgroup = MIGRUPO
03         netbios name = MILINUX
04         server string =
   Pruebas con Samba
05         security = user
06         wins support = yes
07         os level = 33
08         local master = yes
09
10         winbind use default
   domain = yes
11         winbind separator = /
12
13 [datos]
14         path =
   /usr/local/datos
15         comment = Mis datos
16         writable = yes
```

algunas distribuciones que los separan en dos paquetes.

Una vez instalado Samba tenemos que localizar el archivo de configuración. Generalmente está en \texttt{/etc/smb.conf}. El fichero de configuración de Samba es muy complejo debido a la cantidad de opciones que ha ido acumulando con el tiempo. Solo veremos un conjunto de esas opciones, pero nos permitirán compartir una serie de directorios con máquinas Windows.

smb.conf

La sintaxis del fichero de configuración de Samba, el fichero *smb.conf*, no es muy complicada. Se divide en secciones, y cada una de ellas tiene un nombre. Algunas secciones son obligatorias y tienen nombres específicos mientras que otras son opcionales.

El aspecto general será así:

```
[sección 1]
     clave1 = valor1
     clave2 = valor2

[sección 2]
     clave3 = valor3
```

Dentro de cada sección, como podemos observar, hay una serie de lineas en las que se relaciona una entrada o clave con un valor. De esta manera establecemos los parámetros en Samba.

Estos ficheros pueden volverse muy grandes, por eso es posible incluir comentarios. Los comentarios comienzan con *;* y se extienden hasta el fin de la línea.

```
[global]
    ; Esta sección es muy➥
importante
    ; ...
```

Configuración Global

La primera sección que debe aparecer es *[global]*. En ella, como podemos ver por el nombre, configuramos el comportamiento global de Samba. Las redes Windows, antes de la llegada de los sistemas Windows NT, se separan en *grupos de trabajo* y cada máquina pertenece a uno y sólo uno. Las máquinas también tienen nombres que podemos ver cuando exploramos los grupos de trabajo. Es lo primero que configuraremos:

```
[global]
     workgroup = MIGRUPO
     netbios name = MILINUX
```

Bueno, ya tenemos nombre y pertenecemos a un grupo. Ahora toca establecer la seguridad. Existen varias maneras de controlar el acceso a un directorio compartido:

- Control por usuario
- Control por máquina
- Control delegado en dominio
- Control delegado en Active Directory

En los dos primeros es nuestra máquina que controla el acceso y en los dos últimos otra máquina. Como buscamos algo sencillo usaremos autentificación basada en usuario. Cuando hacemos esto, la persona que intente acceder a uno de nuestros directorios compartidos verá aparecer una ventana que le preguntará su nombre de usuario y su clave.

Este usuario y esta clave son gestionados por Samba, como veremos luego, pero deben relacionarse con un usuario local de la máquina donde se ejecuta Samba. Éste es el gran problema resuelto por Samba. Cuando un usuario de Windows crea un directorio en uno de nuestros directorios compartidos con Samba... ¿qué permisos y a quién pertenecerá ese directorio?

En Windows el control de permisos y propietarios en los ficheros es mínimo. De hecho ni siquiera es excluyente. Si digo que un fichero pertenece a *Pepe* el usuario *Juan* puede hacer lo que quiera con él. Este sistema tan inseguro fue eliminado por Microsoft al introducir NTFS y el control estricto de permisos en sus sistemas NT y 2000.

Lo que Samba hace es establecer una relación entre el usuario de red Windows y un usuario local. Por ejemplo, podemos relacionar todos los usuarios que accedan al directorio compartido *Finanzas* con el usuario *finanzas* que hemos creado en Linux. Cada fichero en ese directorio tendrá como propietario a *finanzas*, a pesar de que el usuario que lo está haciendo se ha registrado al acceder al directorio como *JoseManuel*. Por tanto, pondremos:

```
security = user
```

Configuraciones Locales

Con sólo 3 parámetros ya hemos definido unas cuantas opciones básicas, ahora

SimbioNet.com
Premium root server hosting

Especialistas en Servidores dedicados!

Promoción code 0630

Si contrata uno de nuestros servidores hasta el 30.06.05 recibirá un 10% de descuento en los 3 primeros meses de contrato.

» Simbioservidor 150
- Instalación GRATIS!*
- Servidor dedicado propio
- 150 GB volumen de tráfico
- Acceso total al root
- Procesador Pentium III, 733 MHz, 256 MB RAM, 10 GB HDD
- Conexión del servidor 100 Mbits

por sólo 35 Euros al mes

» Simbioservidor 450
- Instalación GRATIS!
- Servidor dedicado propio
- 450 GB volumen de tráfico
- Acceso total al root
- Procesador Intel Celeron 2400, 2.4 GHz, 512 MB DDR RAM, 80 GB HDD
- Conexión del servidor 100 Mbits

por sólo 79 Euros al mes

» Simbioservidor 450x
- Instalación GRATIS!
- Servidor dedicado propio
- 450 GB volumen de tráfico
- Acceso total al root
- Procesador Pentium IV, 2.4 GHz, 1 GB DDR RAM, 1 x 80 GB HDD
- Conexión del servidor 100 Mbits

por sólo 99 Euros al mes

*sólo por contrato anual.
Todos nuestros precios no incluyen el IVA del 16%

Muchos afirman que tienen una buena conectividad, nosotros se lo garantizamos. Compruébelo pregunte por nuestros servidores de prueba!

SimbioNet le ofrece toda una gama de productos para cubrir todas sus necesidades al realizar sus proyectos en Internet. Contamos con herramientas de fácil manejo, cómo un servicio eficaz de atención al cliente.

Nuestros clientes alojan desde páginas publicitarias, aplicaciones especiales con base de datos, portales de busqueda, desarrollo de aplicaciones bajo PHP, Perl, etc., hasta servidores de juegos.

Contáctenos bajo:

Tel: +34 911516959
Fax: +34 912704230
Email: comercial@simbionet.com
http://www.simbionet.com

vamos a compartir algo. Digamos que hemos creado el directorio \texttt{/usr/local/datos} y queremos que otros puedan acceder a él desde sus máquinas Windows.

Tenemos que crear una sección para este directorio, la llamaremos *[datos]*. Todo directorio compartido en una red Windows, *share* en argot Microsoft, debe tener un comentario que lo defina. Así que pondremos uno:

Cuadro 2: Creación del usuario de prueba

```
01 [josemaria@localhost josema-
   ria]# pdbedit -a prueba
02 new password:
03 retype new password:
04 Unix username:        prueba
05 NT username:
06 Account Flags:        [U
   ]
07 User SID:
   S-1-5-21-2193370309-2470947842
   -1102485009-2004
08 Primary Group SID:
   S-1-5-21-2193370309-2470947842
   -1102485009-2005
09 Full Name:
10 Home Directory:       \\mili-
   nux\prueba
11 HomeDir Drive:
12 Logon Script:
13 Profile Path:         \\mili-
   nux\prueba\profile
14 Domain:               MILINUX
15 Account desc:
16 Workstations:
17 Munged dial:
18 Logon time:           0
19 Logoff time:          Fri, 13
   Dec 1901 21:45:51 GMT
20 Kickoff time:         Fri, 13
   Dec 1901 21:45:51 GMT
21 Password last set:    Thu, 28
   Apr 2005 09:35:12 GMT
22 Password can change:  Thu, 28
   Apr 2005 09:35:12 GMT
23 Password must change: Fri, 13
   Dec 1901 21:45:51 GMT
24 Last bad password   : 0
25 Bad password count  : 0
26 Logon hours         :
   FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
   FFFFFFFFFFF
27 [josemaria@localhost josema-
   ria]#
```

```
[datos]      comment = Mis➥
datos compartidos
```

Si ejecutásemos el servidor de Samba ahora aparecería una máquina llamada *MILINUX* en el grupo de trabajo *MIGRUPO*. Podríamos entrar en ella, y veríamos una carpeta *datos* pero no podríamos entrar en ella.

¿Qué nos falta? Pues el sitio en el que realmente existe esa carpeta. El famoso "*What you see is what you get*" (*Lo que ves es lo que tienes*) no se aplica al mundo de Samba ;). A pesar de ver una carpeta compartida *datos*, esa carpeta no existe. Al menos hasta que nosotros lo configuremos correctamente. Esto se hace mediante el parámetro *path*:

```
path = /usr/local/datos
```

Ahora sí será posible acceder, pero antes tenemos que configurar el usuario o usuarios que podrán acceder a ella. Cuando realizamos la configuración global establecimos criterios que afectan a todos los recursos compartidos, a menos que se especifique algo más concreto en los mismo.

El resto de parámetros, que podemos observar en el Cuadro 1, son para permitir el uso de *WINS* (una especie de DNS que usa Microsoft) y para indicar el "tipo de Windows" que somos (en este caso un Windows NT Server).

Samba nos da la posibilidad de usar gran cantidad de mecanismos para guardar a los usuarios. Tenemos desde simples ficheros de texto donde listamos qué usuario local corresponde con qué usuarios de Samba hasta bases de datos como Postgres o incluso LDAP. También podemos usar un mecanismo que el propio Samba nos proporciona usando una especie de base de datos de usuarios. En Samba4 habrá un enfoque unificado para este tema.

Como buscamos simplicidad, no especificaremos el *backend* para almacenar los usuarios, lo que significa que dejaremos que sea Samba quien lo elija.

Primer Arranque

Y ahora, después de tanta ceremonia, vamos a arrancar el servidor de Samba y a realizar unos cuantos experimentos.

Para ello ejecutaremos el servidor de Samba, que de nuevo depende de la distribución de Linux que usemos. Generalmente requerirá ejecutar el daemon *smbd*, en el caso de Mandrake consigue ejecutando como root:

```
# /etc/init.d/smb start
```

Con esto ya deberíamos tener el servidor de Samba funcionando, pero no hemos creado usuarios Samba. Este proceso es muy simple, se realiza empleando el comando *pdbedit* que viene con Samba (ver cuadro "Creación del usuario prueba"):

He puesto toda la salida para que no os asustéis al verla. Solo es información de configuración para ese usuario, en nuestro caso la configuración por definición. El usuario *prueba* debe existir previamente en Linux, en caso contrario tendremos que indicarlo al ejecutar *pdbedit* de manera que pueda relacionar el usuario Samba con algún usuario de Linux.

Es necesario darle permisos al directorio *[datos]* para que el usuario correspondiente en Linux a "prueba" (en nuestro caso también se llamará "prueba") pueda escribir sobre él. Con esto ya tenemos la configuración básica. Ahora vamos a comprobar que todo está bien. Vamos a listar los servicios que ofrecemos (ver cuadro "Consulta a nuestro propios servidor").

Podemos ver como aparece el directorio *datos* que compartimos, pero también otros recursos como *IPC$* o *ADMIN$*. No nos debemos preocupar por ellos, entrar en los detalles de su utilidad ¡nos llevaría casi un libro!

Ahora vamos a realizar una prueba accediendo por red al directorio compartido *datos* y copiando algo en su interior. Como se puede ver en las Figuras 2 y 3, nuestro ordenador con Samba y el directorio aparecen dentro de la red de Windows como el resto. Cuando intentamos acceder nos saldrá una pantalla de *Login* donde tendremos que registrarnos como usuario *prueba*.

Y ya podemos crear, modificar, borrar y copiar ficheros en nuestro directorio compartido desde una máquina Windows. Si queremos tener un control más exhaustivo, por ejemplo permitir que algunos usuarios solo puedan leer mientras otros tengan control total, deberemos especificarlo en *smb.conf*. La manera más sencilla es hacer que el directorio compartido solo pueda ser leído:

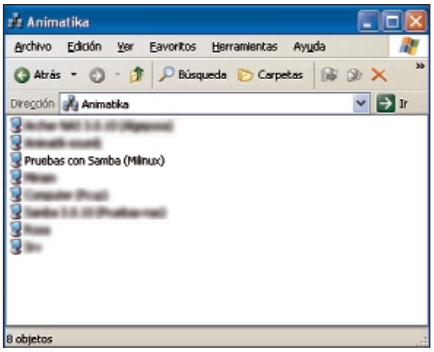

Figura 2: Vemos a nuestro equipo, Milinux, dentro de la red de Windows.

```
read only = yes
 ;      o
 writable = no
```

La opción *writable = no* es equivalente a *read only = yes*. Pero si ponemos *writable = yes* o *read only = no* entonces permitimos tanto la lectura como la escritura. Es un poco lioso por lo que recomiendo que se use *writable* o *read only* y no mezclar. Podemos ser más restrictivos solo permitir que puedan leer el directorio algunos usuarios.

```
valid users = prueba
```

De esta manera sólo el usuario *prueba* puede acceder al directorio que hemos compartido. Podríamos entrar en más detalles, pero requeriría muchas más páginas. Con esta configuración mínima podemos ya compartir con los ordenadores de una red Windows uno o varios directorios y controlar el acceso desde nuestra máquina.

Active Directory

Microsoft ha realizado una gran campaña de publicidad alrededor de su tecnología Active Directory y, la verdad, es que no conozco mucha gente que sepa lo que es realmente esa cosa llamada "Active Directory".

Active Directory es un sistema que permite gestionar el acceso a los *objetos* de una red de manera centralizada. Estos *objetos* pueden ser muchas cosas: usuarios, máquinas, impresoras o ficheros.

Ahora imaginemos una red de cierto tamaño, digamos 100 máquinas. Tenemos que administrarlas y entre nuestras funciones estaría el gestionar el acceso a los ficheros de todas las máquinas. Ya puestos no estaría mal que me pudiese sentar en cualquiera de las 100 máquinas, introducir mis datos y que allí apareciese mi escritorio.

Esto puede ser una pesadilla para cualquier administrador de sistemas. Pero esto también es lo que Active Directory promete realizar. Para ello Active Directory necesita realizar varias funciones:

- Tiene que proporcionar un mecanismo para mantener seguras las comunicaciones.
- Debe llevar un control de los usuarios del sistema.
- Debe llevar un control de las máquinas de la red.
- Debe llevar un control de los ficheros en cada máquina.

Estas funciones las realizan varias máquinas en las redes UNIX. Por ejemplo, la identificación distribuida se realiza con NIS/NIS+ y el control de las máquinas de la red con una mezcla de DHCP y DNS. Las máquinas Active Directory hacen todo estoy y también gestionan otros recursos como la sincronización horaria (NTP).

Configuración de Samba para Active Directory

El uso de Active Directory y Samba es un tema candente en muchos foros. La idea de poder delegar la autenticación en una máquina Active Directory hace que Samba entre en la nueva era de las redes Microsoft.

Antes dimos una descripción un poco simplista sobre lo que es y hace Active

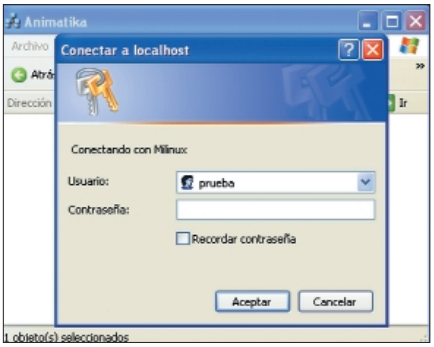

Figura 3: Cuando nos pida la clave tenemos que darle la que introducimos al crear al usuario "prueba".

Directory, la realidad es mucho más complicada. Active Directory se basa en un diseño enorme con el que Microsoft pretende atacar el problema de la administración de redes cada vez más grandes. El equipo de Samba siempre ha tenido en la mira a Active Directory, pero una serie de problemas tecnológicos les han apartado de la simulación total.

El primer problema es el propio Samba. Con un código fuente que adolece de más de 10 años de desarrollo continuo no se pueden hacer demasiados experimentos. Por ello el equipo se ha centrado en Samba4 que incorpora la reescritura desde cero, con un diseño más lógico, de la mayoría de código.

Aún así han ido introduciendo poco a poco en versión 3 algunas de las tecnologías que permiten al sistema interactuar con Active Directory.

Active Directory deja absolutamente anticuado al anterior diseño de Microsoft.

Cuadro 3: Consulta a nuestro propio servidor

```
[josemaria@localhost lib]# smbclient -L //localhost -U prueba
Password:
Domain=[MILINUX] OS=[Unix] Server=[Samba 3.0.15pre2-SVN-build-]
      Sharename       Type      Comment
      ---------       ----      -------
       datos           Disk      Mis datos
       IPC$            IPC       IPC Service (Samba
                                3.0.15pre2-SVN-build-)
       ADMIN$          IPC       IPC Service (Samba
                                3.0.15pre2-SVN-build-)
Domain=[MILINUX] OS=[Unix] Server=[Samba 3.0.15pre2-SVN-build-]
      Server               Comment
      ---------            -------
      Workgroup            Master
      ---------            -------
[josemaria@localhost lib]#
```

El sistema de autentificación y listado de recursos es nuevo. Esto ha supuesto un reto, puesto que el equipo de Samba localiza los cambios filtrando los paquetes de la red cuando las máquinas Windows están realizando operaciones.

La primera sorpresa, aunque fue ampliamente publicitado por Microsoft, fue el uso de Kerberos como protocolo de autentificación. Por ello es muy importante que tengamos alguna de las implementaciones de Kerberos instaladas. La configuración de cada una de ellas es distinta, pero el fin es el mismo: hacer que la máquina Active Directory sea la entidad emisora de certificados.

Una vez que Kerberos esté correctamente configurado pasaremos a configurar nuestro servidor Samba. Es importante tener las versión más moderna posible de Samba. Los cambios en el código fuente se están sucediendo con rapidez durante los últimos meses.

El fichero de configuración tendrá la forma que se ve en el cuadro "Configuración para Active Directory":

Como podemos ver la configuración de *[datos]* no ha cambiado. Son los parámetros globales, y los de autentificación en particular, los que tenemos que cambiar. El modo de autentificación, el parámetro *security*, pasa a ser *ads*.

Este modo es temporal, aunque probablemente esté en Samba3 durante un buen tiempo, y se debe a que Samba aún no es capaz de auto-detectar la presencia de una servidor Active Directory.

El *realm* es el mismo que establezcamos en la configuración de Kerberos y se suele corresponder con el dominio que establezca Active Directory, mientras que *password**server* tiene que ser la IP o nombre de la máquina que se encarga de las autentificaciones en nuestra red Active Directory.

Con esta simple configuración conseguimos que nuestro Samba esté preparado para funcionar con Active Directory, así que volvemos a arrancar Samba.

Existe un paso intermedio aún. Aunque estemos configurados para funcionar con Active Directory tenemos que unirnos al dominio. Para ello ejecutamos:

```
[josemaria@localhost ~]# net ads join -U Administrador@MIDOMINIO.COM
password:
[josemaria@localhost ~]#
```

Cuando realizamos esta acción nuestra máquina se registra en el servidor Active Directory y debería aparecer, puede tardar unos segundos debido al cacheo que realiza Active Directory, en el dominio configurado. Si todo ha ido bien, al ejecutar *net ads user -U Administrador@MIDOMINIO.COM* deberíamos obtener un listado con todos los usuarios de Active Directory.

Con *net ads info -U Administrador@MIDOMINIO.COM* podremos obtener información genérica sobre el servidor Active Directory.

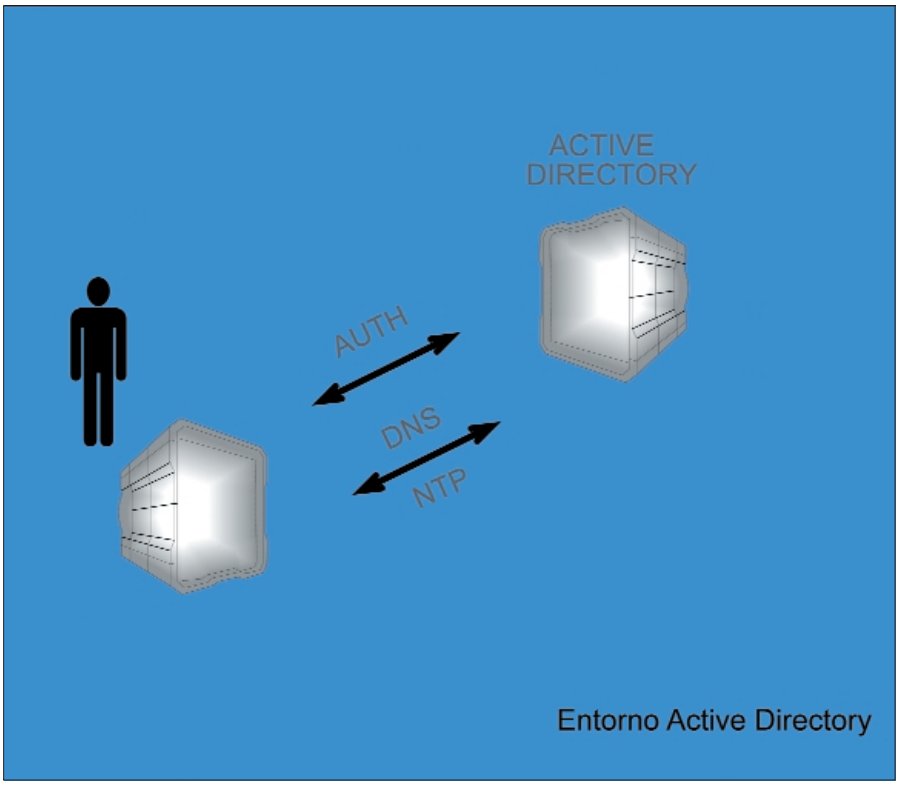

Figura 4: Tipos de interacción con Active Directory.

Cuadro 4: Configuracion para Active Directory

```
01 [global]
02         workgroup = MiDominio
03         netbios name =
   Pruebas-AD
04         security = ads
05         wins support = yes
06         winbind use default
   domain = no
07         realm = midominio.com
08         password server =
   srv.midominio.com
09
10 [datos]
11         path =
   /usr/local/datos
12         comment = Directorio
   de prueba
13         writable = yes
```

Conclusión

Aunque el soporte de Samba3 es muy reciente, y por tanto posee fallos, el proyecto Samba se mueve a pasos agigantados hacia la emulación total de un servidor Active Directory. A Samba4 aún le queda tiempo, dicen que un año y medio, pero puede que esté ahí cuando Microsoft lance una versión para servidor de su famoso Longhorn. Entre la gente que querrá obtener la primera copia seguro que habrá unos cuantos colaboradores de Samba. ■

EL AUTOR

José María Ruiz es programador de sistemas y director de proyectos en Animatika, una empresa dedicada al software libre, mientras intenta acabar su proyecto fin de carrera en Ingeniería Técnica Informática de Sistemas.