IURRETA INSTITUTUA
Goi-mailako Lanbide-Heziketako Berariazko Institutua
2005

EUSKO JAURLARITZA
GOBIERNO VASCO
HEZKUNTZA UNIBERTSITATE ETA IKERKETA SAILA
DEPARTAMENTO DE EDUCACIÓN UNIVERSIDADES E INVESTIGACIÓN

INTEGRACION LINUX WINDOWS

Parte1: Integración de Linux en AD

Versión: 1.0

Alfredo Barrainkua Zallo

Mayo del 2007

SOME RIGHTS RESERVED CreativeCommons - ShareAlike
Lizentzia laburpena: English Castellano

Indice

1. Introducción

Actualmente parece que la tendencia en el mundo de los PCs de escritorio es a la diversificación. esto hace que sea más frecuente encontrarse con entornos mixtos. A su vez, en redes con gran número de clientes Windows, éstos se encuentran englobados en ámbitos de seguridad, con un alto coste en licencias. Vamos a abordar en este curso, posibles soluciones a estos dos problemas.

En la primera parte del curso vamos ver la integración de clientes Linux en dominios windows con Active Directory. Se van a abordar los temas de la autentificación, la compartición de recursos y la autorización del uso de dispositivos de almacenamiento. No se va a intentar integrar en más profundidad, con más personalización, pues varían ya en gran manera los objetivos a conseguir y los tipos de configuraciones a considerar. En esta documentación vamos a utilizar **NIRESERVER** como nombre del servidor, **NIREDOMAIN** como nombre **NETBIOS** del dominio y **192.168.33.44** como dirección IP del controlador de dominio. El nombre DNS del dominio es **niredomain.net**, y el reino kerberos **NIREDOMAIN.NET**.

2. Instalación de Ubuntu

La instalación de Ubuntu comienza con el arranque del PC desde el CD-ROM. Cuando aparece el menú inicial, pulsamos **F2** y seleccionamos el idioma español. Al final del arranque del **LiveCD** nos encontramos con un sistema funcional de **Ubuntu**. En el escritorio se encuentra un icono llamado **instalar**. Haciendo doble clic en dicho icono comienza el proceso de instalación a disco.

Seleccionamos:

Idioma -> Español
Zona horaria-> España, Madrid
Teclado -> Spain, Spain. Lo probamos

Detección del hardware....
Método de particionado: Manual
En el ESPACIO LIBRE:
- Crear partición nueva.
- Tamaño de la partición: 500 MB
- Ubicación de la nueva partición: Principio
- Punto de montaje: /boot
- Detección del hardware....

En el ESPACIO LIBRE:
- Crear partición nueva.
- Tamaño de la partición: 1 GB
- Ubicación de la nueva partición: Principio
- Utilizado como: Área de intercambio
- Detección del hardware....

En el ESPACIO LIBRE:
- Crear partición nueva.
- Tamaño de la partición: Resto
- Punto de montaje: /
- Detección del hardware....

Finalizar el particionamiento y escribir los cambios en el disco.
Creación del usuario inicial
- Nombre usuario inicial Usuario inicial
- Nombre de inicio de sesión: iurreta
- Contraseña: iurreta (2 veces)
- Nombre del equipo: I2UBPCxx

Copiando paquetes....

Instalación completada. Reiniciar ahora.

2.1. Estableciendo los repositorios a utilizar

Para que la instalación de paquetes sea más ágil, vamos a utilizar el **proxy apt** que tenemos en la escuela. Para ello, en **/etc/apt/sources.list** vamos a poner lo siquiente:

```
deb http://10.22.1.9:9999/ubuntu feisty main restricted universe multiverse
deb http://10.22.1.9:9999/ubuntu feisty-updates main restricted universe multiverse
deb http://10.22.1.9:9999/ubuntu feisty-backports main restricted universe
multiverse
deb http://10.22.1.9:9999/ubuntu feisty-security main restricted universe
multiverse
```

Ahora vamos a actualizar la base se datos y a actualizar los paquetes que se hayan modificado desde la publicación del CD de instalación.

```
      apt-get update
      apt-get upgrade
```

2.2. Instalación de paquetes adicionales

Vamos a instalar paquetes adicionales a la instalación por defecto. Primero vamos a instalar todos los paquetes de OpenOffice y de los escritorios GNOME y KDE para que las aplicaciones puedan ser utilizadas en Euskera y Castellano.

```
      apt-get install -y openoffice.org-help-es openoffice.org-l10n-es
#     apt-get install -y openoffice.org-help-eu openoffice.org-l10n-eu
      apt-get install -y myspell-es aspell-es
      apt-get install -y language-support-es language-support-eu
      apt-get install -y language-pack-es language-pack-eu
      apt-get install -y language-pack-gnome-es language-pack-gnome-eu
      apt-get install -y language-pack-kde-es language-pack-kde-eu
      apt-get install -y kde-i18n-es kde-i18n-eu khelpcenter
```

Ahora vamos a instalar otros paquetes adicionales como las aplicaciones de dibujo **Dia Inkscape** y el gestor de proyectos **Planner**. También vamos a instalar el demonio de tiempo ntp, ntpdate, mc y el descompresor arj.

```
      apt-get install -y ntp ntpdate
      apt-get install -y inkscape dia dia-gnome planner
      apt-get install -y fuse-utils
      apt-get install -y mc arj
```

Ahora vamos a instalar el cliente de correo **Thunderbird**, pero en modo gráfico, con

synaptic.

Elegir los siguientes paquetes:

mozilla-thunderbird
thunderbird-locale-eu
thunderbird-locale-es-es
mozilla-thunderbird-enigmail

Con esto tenemos unos paquetes mínimos para trabajar, y hemos aprendido a instalarlos.

3. PAM (Pluggable Authentication Modules)

PAM es un sistema de módulos intercambiables que proporciona una interfaz entre las distintas aplicaciones y los diferentes métodos de autentificación. Esto soluciona el problema de que una vez definido un sistema de autentificación no es fácil cambiarlo. Mediante PAM podemos comunicar las aplicaciones con los métodos de autentificación que deseemos de una forma transparente. El uso de PAM se realiza a través de librerías compartidas que implementan las políticas de cuentas, seguridad, etc. Los módulos PAM se instalan en el directorio **/lib/security**. Normalmente, el módulo más utilizado es **pam_unix.so**.

PAM afecta tanto al proceso de autentificación como al de autorización. La autentificación es el proceso de determinar la identidad de quién es quien dice ser. La autorixzación es el proceso de determinar qué se nos permite hacer, una vez establecida la identidad.

La aplicaciones pueden solicitar y preguntar a pam, cosas como:

- Es esta la clave de este usuario?
- Cambia la clave de este usuario de la forma determinada
- Está autorizado este usuario para conectarse a las 10:00 horas?
- Puede ese usuario conectarse desde ese lugar?
- Al entrar en sesión, añade a ese usuario a este otro grupo
- Al conectarse, monta a ese usuario estas conexiones de red

3.1. Configurando PAM

Cada aplicación que usa el sistema PAM, tiene su fichero de configuración en el directorio **/etc/pam.d**. Podemos encontrar ahí cdron, gdm, sudo, samba, ...

La sintaxis general de un fichero de configuración es:

tipo-modulo flag-control módulo parámetros

Hay cuatro tipos de módulos

auth	Estos módulos se utilizan para realizar la autentificación. Pueden buscar y verificar el password en los ficheros locales, servidores LDAP, NIS, etc.
account	Se utilizan para realizar ciertas funciones relacionadas con las cuentas de usuario, pero no relacionadas con la autentificación. Por ejemplo, gestión de la expiración de la cuenta, uso de su, ...
session	Se proporcionan funciones de gestión de la sesión antes de que un usuario acceda a un servicio, o después de hacerlo. Pueden realizarse chequeos de correo nuevo, montar el directorio home del usuario, ...
password	Se utiliza para modificar el password del usuario, cuando se requieren algún tipo de credenciales de usuario para ello. Especifica además la forma y condiciones para realizarlo.

Cada tipo de módulo puede aceptar uno de los cuatro flags que están definidos para determinar la forma en que un módulo interactúa con los otros.

Los cuatro flags de control:

required	Indica que este módulo debe tener éxito para que la autentificación o autorización tengan éxito. El control se devuelve a la aplicación, una vez de que todos los módulos han sido invocados
sufficient	Indica que el éxito de este módulo es suficiente para que la autentificación prospere, suponiendo que los módulos que le han precedido no han fallado. En caso de que tenga éxito, ningún otro módulo requerido es evaluado, y devuelve el control a a aplicación. Si falla, el proceso continúa con los módulos siguientes. El fallo del módulo no deniega el acceso.
optional	Indica que el éxito o fallo del módulo no tiene efecto en el estatus del retorno a la aplicación. Hay una excepción a esto. Si ningún otro módulo devuelve ningún estatus, el éxito o fallo de este módulo determina el éxito o fallo de la autentificación.
requisite	Indica que el módulo deberá tener éxito para que se produzca la autentificación. Si falla, el control se pasa a la aplicación indicando el fallo.

Los argumentos que soporta un módulo varían dependiendo del módulo, pero hay una serie de ellos que son soportados por todos los módulos.

debug	Activa el nivel debug en los logs de syslog
no-warn	Deshabilita el registro de los fallos en los logs
use_first_pass	Indica al módulo que utilice el password introducido para el módulo previo. Si falla, se notifica como fallo.

try_first_pass	Indica al módulo que intente primeramente utilizar el password introducido para el módulo previo. En caso de fallo, solicita una nueva contraseña.

3.2. Apilando los módulos

Si apilamos los módulos necesarios para cierta tarea, hacemos que los usuarios sean evaluados a través de múltiples servicios. Estos servicios pueden ser de autentificación o de limitación. Veamos un ejemplo típico:

```
auth  required    pam_unix.so
auth  required    pam_securetty.so
auth  required    pam_nologin.so
```

Cualquier intento de autentificación deberá ser aprobado por los tres módulos para que la autentificación tenga éxito.

El módulo **pam_unix** realiza la autentificación estándar de usuario, a través de los ficheros del sistema (**/etc/passwd**, **/etc/shadow**) o **NIS**.

El módulo **pam_securetty** hace que el login de root falle, si el terminal tty no está incluido en el fichero **/etc/securetty**. Esto es una forma de que el administrador limite el acceso como root a través de ciertos sistemas.

El módulo **pam_nologin** mira la existencia del fichero **/etc/security/access.conf**. Si el usuario está en dicho fichero, la autentificación se le es denegada.

Los módulos se procesan siempre en orden. El primero en aparecer en el listado, es el primero en ser procesado. Está permitida la inclusión de unos ficheros en otros para organizar más flexiblemente el sistema. Para ello se utiliza la directiva “**@include**”.

4. NSS (Name Service Switch)

NSS especifica los ficheros y servicios que se han de utilizar para obtener información. La información puede ser de usuarios, hosts, servicios, etc. Por ejemplo, podemos indicar que utilice los ficheros del sistema, NIS DNS o WINS para realizar la resolución de nombres de hosts. Podemos indicarle que utilice uno o varios de los sistemas, y el orden de búsqueda. El fichero de configuración es **/etc/nsswitch.conf**. Este es el aspecto de dicho fichero:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat
group:          compat
shadow:         compat

hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

La librería **glibc** utiliza los ficheros **/lib/libnss_SERVICE.so.X** para cada servicio que usamos. Estos son los ficheros en un sistema Ubuntu 7.04:

```
/lib/libnss_compat-2.5.so
/lib/libnss_compat.so.2 -> libnss_compat-2.5.so
/lib/libnss_dns-2.5.so
/lib/libnss_dns.so.2 -> libnss_dns-2.5.so
/lib/libnss_files-2.5.so
/lib/libnss_files.so.2 -> libnss_files-2.5.so
/lib/libnss_hesiod-2.5.so
/lib/libnss_hesiod.so.2 -> libnss_hesiod-2.5.so
/lib/libnss_mdns4_minimal.so.2
/lib/libnss_mdns4.so.2
```

```
/lib/libnss_mdns6_minimal.so.2
/lib/libnss_mdns6.so.2
/lib/libnss_mdns_minimal.so.2
/lib/libnss_mdns.so.2
/lib/libnss_nis-2.5.so
/lib/libnss_nisplus-2.5.so
/lib/libnss_nisplus.so.2 -> libnss_nisplus-2.5.so
/lib/libnss_nis.so.2 -> libnss_nis-2.5.so
```

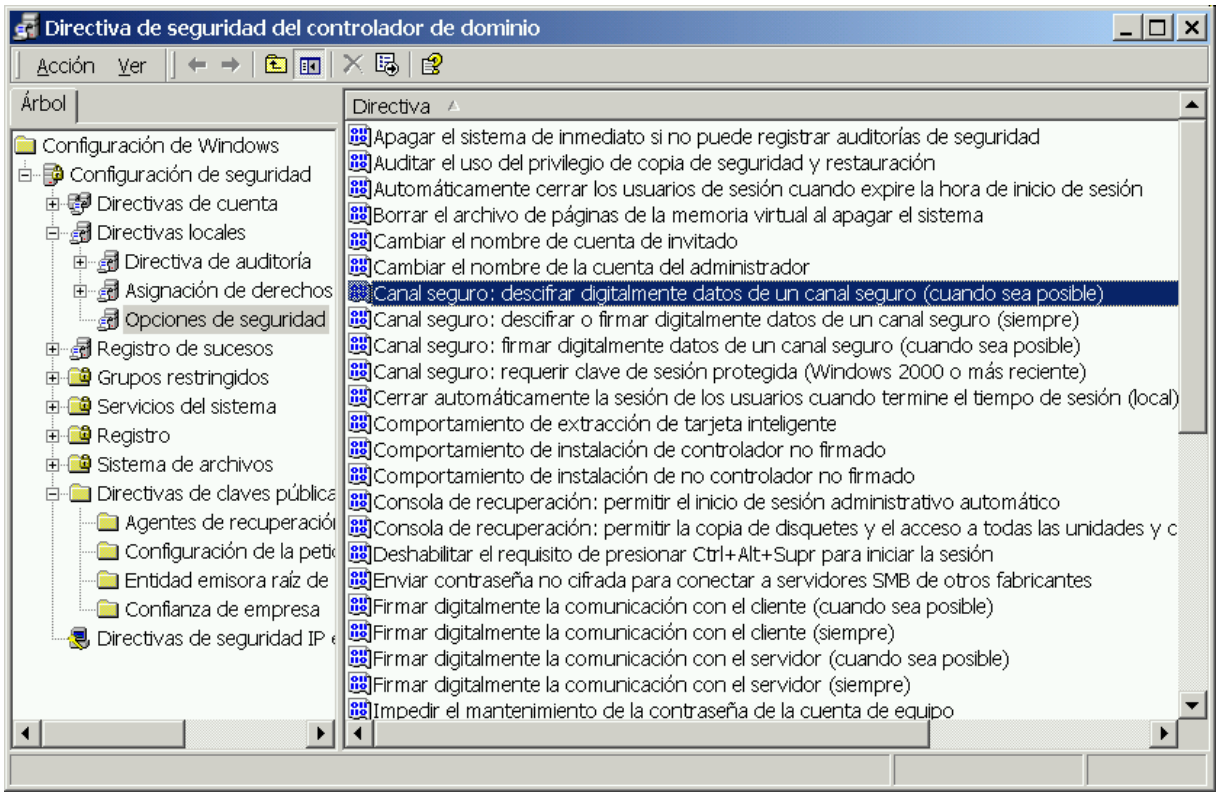
5. Autentificando contra AD

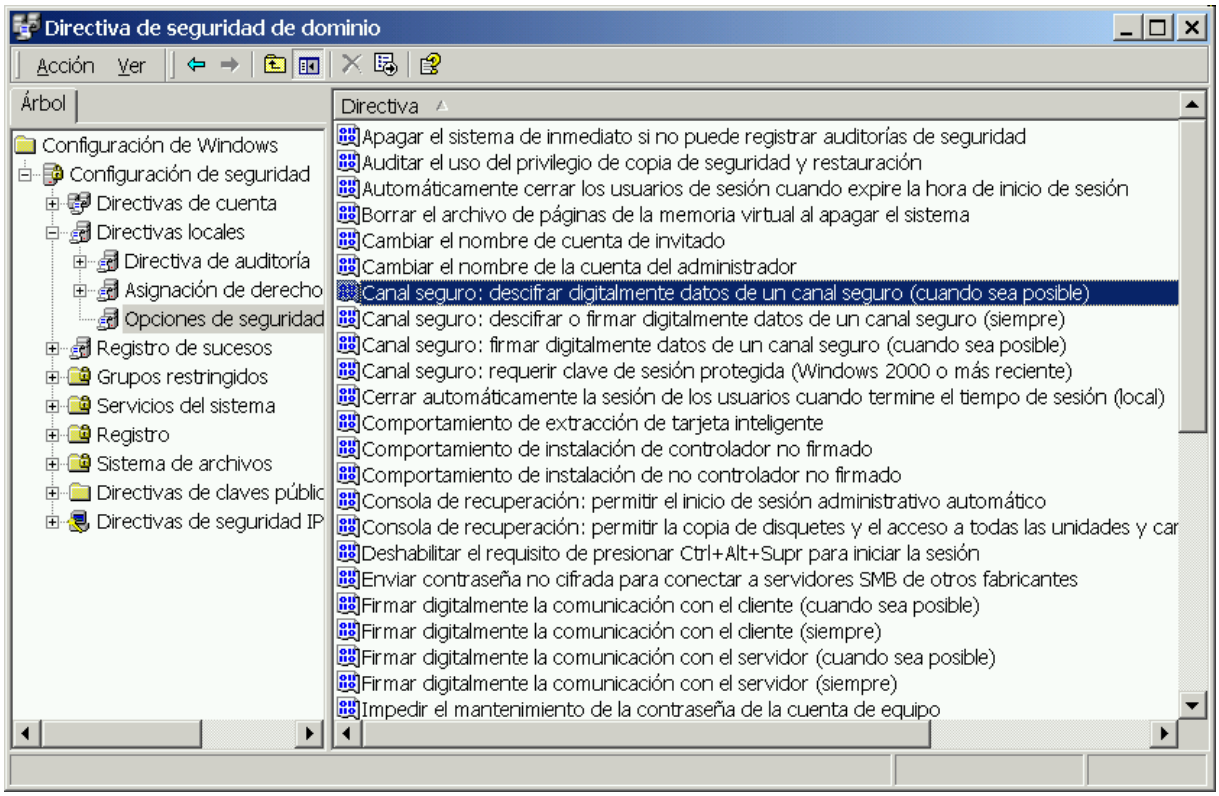
Vamos a entrar ya en la parte práctica del tema. Vamos a instalar los paquetes necesarios, y a configurar nuestro sistema para realizar la autentificación en el directorio activo. También vamos a montar carpetas compartidas e incluir a los usuarios, en los grupos que tienen permisos para montar unidades de almacenamiento.

5.1. Preparando AD en Windows 2000 Server

Hay un par de detalles que debemos de tener en cuenta en la configuración del servidor Windows.

Primero, debemos permitir las conexiones no cifradas en las Directivas de seguridad del controlador de dominio y del dominio. En Directivas de seguridad del controlador de dominio\Configuración de Windows\Configuración de seguridad\Opciones de seguridad, buscamos “Canal seguro: descifrar o firmar digitalmente datos de un canal seguro (siempre)” y “Canal seguro: firmar digitalmente datos de un canal seguro (cuando sea posible). Definimos estas dos políticas como deshabilitadas. Lo mismo hacemos para las directivas de seguridad del dominio. En estas dos imágenes podemos verlo.





Aplicamos los cambios inmediatamente. Para ello, debemos entrar en modo terminal y ejecutar el siguiente comando:

```
gpupdate
```

NOTAS:

1- En Windows 2000 Server, si no está definida la política de seguridad (opción por defecto) también funciona.

2- Es posible que en futuras versiones de Samba no sea necesario hacer esto. Comprobarlo.

5.2. Instalación de paquetes en Ubuntu

Necesitamos los siguientes paquetes:

kerberos	Librerías de soporte del protocolo kerberos
samba	Librerías para soporte del protocolo SMB
winbind	Autentificación y acceso a servici0os usando el protocolo SMB
smbfs	Sistema de ficheros virtual en espacio de usuario para el protocolo SMB
libpam_mount	Librerías PAM para montaje de volúmenes de red

Necesitamos también otras librerías PAM (**group**, **mount**, **mkhomedir**), pero Ubuntu las instala siempre. Si estamos utilizando otra distribución quizás las tengamos que instalar. Vamos a instalar los paquetes que no tenemos instalados..

```
apt-get install krb5-user winbind samba smbfs libpam_mount
```

5.3. Configuración de Kerberos

Kerberos es un sistema de autentificación desarrollado en el MIT. Es el sistema que utilizan los dominios Windows desde Windows 2000.

Tenemos que configurar este sistema a través de su fichero de configuración **/etc/krb5.conf**. Veámos cómo queda:

```
[libdefaults]
      default_realm = NIREDOMAIN.NET

      ticket_lifetime = 24000
      kdc_timesync = 1
      ccache_type = 4
      forwardable = true
      proxiable = true

      dns_lookuo_realm = false
      dns_lookup_kdc = false

[realms]

      NIREDOMAIN.NET = {
            kdc = nireserver.niredomain.net
            admin_server = nireserver.niredomain.net
            default_domain = niredomain.net
      }

[domain_realm]
      .niredomain.net = NIREDOMAIN.NET
      niredomain.net = NIREDOMAIN.NET
```

5.4. Configuración de Samba

Samba es un servidor que utiliza el protocolo **SMB**, y que replica la funcionalidad de un servidor y controlador de dominio Windows. No vamos a utilizar aquí las capacidades de servidor de Samba, pero sí una parte de sus capacidades de utilizar el protocolo SMB. La utilidad **winbind**, que es parte de **samba**, nos va a permitir hablar con el servidor Active Directory para la búsqueda de información de usuarios, grupos, etc.

El fichero de configuración de samba se encuentra en **/etc/samba/smb.conf**. Este fichero trae por defecto, configurados muchos parámetros de configuración. Nosotros

vamos a utilizar solamente unos cuantos. Este es el aspecto de este fichero para nuestro uso:

```
[global]
    netbios name = NIRESERVER
    workgroup = NIREDOMAIN
    realm = NIREDOMAIN.NET
    security = ads
    password server = nireserver.niredomain.net

    winbind use default domain = yes
    winbind separator = +
    winbind enum users = no
    winbind enum groups = no
    idmap uid = 10000-20000
    idmap gid = 10000-20000

    template homedir = /home/%D/%U
    template shell = /bin/bash

    client use spnego = yes
    domain master = no

    log file = /var/log/samba/log.%m
    max log size = 1000
    syslog = 0
```

Ahora reiniciamos el servicio winbind.

```
/etc/init.d/winbind restart
```

5.5. Uniendo el host al dominio

Para unir el host al dominio Windows, hemos de realizar unos pequeños preparativos aún. Kerberos es un sistema exigente en cuanto a la sincronización horaria. Así pues, hemos de tomar como referencia el propio controlador de dominio. Ca,biemo0s el fichero **/etc/ntp.conf**, y hagamos que se utilice como servidor horario nuestro controlador de dominio.

```
server nireserver.niredomain.net
```

Vamos a configurar también el servidor DNS a utilizar. Vamos a indicarle que utilice el controlador de dominio Windows como primer resolver, En el fichero **/etc/resolv.conf** deberá aparecer la dirección IP de nuestro controlador de dominio y el nombre del dominio como puede verse en el ejemplo siguiente:

```
search niredomain.net
nameserver 192.168.33.44
```

Para crear los homes de los usuarios del dominio la primera vez que se autentifican, necesitamos un directorio con el nombre del dominio. Con el nombre **NETBIOS** concretamente. Vamos a crearlo con los permisos adecuados:

```
mkdir /home/NIREDOMAIN
chmod 777 /home/NIREDOMAIN
```

Vamos ahora a comprobar si podemos conectarnos al servicio de distribución de **tickets** de kerberos. Utilizaremos una cuenta de administrador de dominio:

```
kinit domainadmin@@NIREDOMAIN.NET
```

Si no hay errores comprobamos los tickets kerberos que tenemos

```
klist
```

Si existe el fichero **/etc/samba/secrets.tdb** lo borramos. Este fichero se crea al unirse el host al dominio.

```
rm /etc/samba/secrets.tdb
```

Si parece que el sistema funciona, unimos el host al dominio. Para ello vamos a utilizar el comando **net** de las utilidades de samba:

```
net ads join -U domainadmin@@NIREDOMAIN.NET
```

Si todo ha ido bien, podremos listar los usuarios y grupos del dominio con los comandos:

```
wbinfo -u
wbinfo -g
```

5.6. Configuración de NSS

Hemos de añadir el soporte winbind para los usuarios grupos y passwords a NSS. Además, la resolución de nombres de hosts utilizará también el sistema **wins**. El fichero de configuración **/etc/nsswitch.conf**, quedará tal como:

```
passwd:         compat winbind
group:          compat winbind
shadow:         compat winbind

hosts:          files dns wins
networks:       files

protocols:      db files winbind
services:       db files winbind
ethers:         db files
rpc:            db files
```

```
netgroup:       nis winbind
```

Vamos a comprobar el funcionamiento de NSS. Vamos a listar las cuentas de usuario y grupo del directorio.

```
getent passwd
getent group
```

5.7. Configuración de los módulos PAM

Los módulos a modificar son los correspondientes a la autentificación, cuentas, sesiones y contraseñas. También tenemos la posibilidad de utilizar este sistema de autentificación para sudo. Veamos cómo quedan:

/etc/pam.d/common-auth

```
auth optional     pam_group.so
auth sufficient   pam_winbind.so
auth sufficient   pam_unix.so nullok_secure use_first_pass
```

/etc/pam.d/common-account

```
account sufficient      pam_unix.so
account sufficient      pam_winbind.so use_first_pass
```

/etc/pam.d/common-session

```
session required  pam_mkhomedir.so umask=0022 skel=/etc/skel
session required  pam_winbind.so
session required  pam_unix.so use_first_pass
session optional  pam_foreground.so
```

/etc/pam.d/common-password

```
password sufficient     pam_unix.so nullok obscure min=4 max=8 md5
password required       pam_winbind.so use_first_pass
```

/etc/pam.d/sudo

```
auth sufficient   pam_winbind.so
auth required     pam_unix.so use_first_pass
```

Solo nos resta reiniciar la máquina y loguearnos como un usuario del dominio.

5.8. Concediendo derechos sobre el CD-ROM y floppy

Para poder montar y utilizar las unidades de CD-ROM en un sistema Linux, se ha de ser

miembro del grupo cdrom. Lo mismo sucede con la unidad de diskettes. Se ha de ser del grupo floppy. Otro tanto podemos decir de los usuarios de scanners, de sistemas de audio, o impresión, ...

Cuando creamos usuarios en nuestro sistema Linux, podemos añadirlos o no a estos grupos, para administrar sus derechos. En Active Directory no existen estos grupos y no podemos realizar esta gestión basándonos en ellos. Pero tenemos otra solución. Vamos a hacer que todos los usuarios que se autentifiquen sean miembros temporales de estos grupos. Para ello vamos a utilizar un módulo de PAM. El módulo es **pam_group.so**. La configuración de este módulo se realiza en el fichero **/etc/security/group.conf**. Vamos a hacer que todos los usuarios que se autentifiquen por los servicios en modo terminal (login), o a través de los servicios de gestores de displays de KDE (kdm) o GNOME (gdm), por cualquier terminal y a cualquier hora, se añadan a los grupos users, cdrom, floppy, plugdev, audio, video, scanner, ... El aspecto del fichero es el siguiente:

```
login;*;*;Al0000-2400;users,cdrom,floppy,plugdev,audio,dip
gdm;*;*;Al0000-2400;users,cdrom,floppy,plugdev,audio,dip,video,scanner
kdm;*;*;Al0000-2400;users,cdrom,floppy,plugdev,audio,dip,video,scanner
```

La ejecución del módulo pam_group se realiza en la autentificación, como podemos observar en el fichero **/etc/pam.d/common-auth**. Es el primer módulo

5.9. Resolviendo el problema de HAL y dbus

La utilización del mecanismo pam_group funciona perfectamente con Ubuntu 6.06 y 6.10, pero con Ubuntu 7.04 se ha introducido otro mecanismo de montaje de unidades HOT-PLUG. Esto afecta directamente a los PenDrives. El sistema HAL que está en la base de este mecanismo de conexión en caliente, no soporta pam_group. Los motivos que se aducen son relacionados con la seguridad. Debemos modificar el comportamiento de HAL. Concretamente, los permisos que se utilizan por defecto. El fichero de configuración que se utiliza para controlar los permisos de envío de mensajes de eventos del sistema **dbus** está en **/etc/dbus-1/system.d/hal.conf**. Las siguientes líneas han de ser modificadas para que queden de esta forma:

```
<!-- Default policy for the exported interfaces -->
<policy context="default">
  <deny send_interface="org.freedesktop.Hal.Device.SystemPowerManagement"/>
  <deny send_interface="org.freedesktop.Hal.Device.VideoAdapterPM"/>
  <deny send_interface="org.freedesktop.Hal.Device.LaptopPanel"/>
  <allow send_interface="org.freedesktop.Hal.Device.Volume"/>
  <allow send_interface="org.freedesktop.Hal.Device.Volume.Crypto"/>
</policy>
```

5.10. Montando automágicamente los recursos de red

En las redes Unix tradicionales, los directorios personales (homes) de los usuarios se centralizan en un servidor y se comparten en las máquinas a través de **NFS**. En los

sistemas Windows también se hace esto. Estos directorios se exportan como recursos SMB. Para que las máquinas Linux monten estos recursos SMB (**shares**) utilizaremos un módulo PAM. Este módulo es **pam_mount.so**. La configuración de los recursos a montar se realiza en el fichero **/etc/security/pam_mount.conf**. En este fichero hay mucha información. Los volúmenes que deseamos montar los añadiremos al final del fichero. He aquí un ejemplo de la información a añadir:

```
volume * smbfs NIRESERVER &$ /home/NIREDOMAIN/&/ZERB-&
uid=&,gid=&,dmask=0750,codepage=cp850,iocharset=utf8 - -

volume * smbfs NIRESERVER shareak$ /home/NIREDOMAIN/&/ZERB-shareak
uid=&,gid=&,dmask=0750,codepage=cp850,iocharset=utf8 - -

volume * smbfs NIRESERVER eskola$ /home/NIREDOMAIN/&/ZERB-eskola
uid=&,gid=&,dmask=0750,codepage=cp850,iocharset=utf8 - -
```

Las líneas comienzan con la palabra **volume**. SERVER es el nombre del host que que exporta las unidades compartidas SMB. el carácter “&” indica el nombre del usuario. Como opciones utilizaremos el código de página 850 y el juego de caracteres utf-8, entre otras.

Para hacer uso de este mecanismo, necesitamos indicarle a PAM que utilice el módulo **pam_mount**. Lo haremos en los ficheros PAM correspondientes a la autentificación y a la sesión. Después del añadido quedarán de esta manera:

/etc/pam.d/common-auth

```
auth optional     pam_group.so
auth sufficient   pam_winbind.so
auth sufficient   pam_unix.so nullok_secure use_first_pass
auth sufficient    pam_mount.so use_first_pass
```

/etc/pam.d/common-session

```
session required  pam_mkhomedir.so umask=0022 skel=/etc/skel
session required  pam_winbind.so
session required  pam_unix.so use_first_pass
session sufficient      pam_mount.so use_first_pass
session optional  pam_foreground.so
```

NOTA: Este módulo tiene un bug, que hace que nos pida dos veces la contraseña cuando accedemos como un usuario local.

6. Cosillas varias

Hay otras cosillas que pueden interesarnos cambiar. Entre ellas, estará el que root pueda acceder al sistema. Para ello deberemos crearle el password. Como el usuario creado en la instalación haremos:

```
sudo su
passwd
```

Si queremos que root pueda utilizar el interfase gráfico, habilitaremos su sesión en **gdm**. En el fichero de configuración de **gdm** (**/etc/gdm/gdm.conf**), haremos que la siguiente línea aparezca de esta forma:

```
AllowRoot = true
```

También puede ser interesante que cierto grupo de Active Directory pueda ejecutar acciones de root en las máquinas Linux del dominio. Para ello creamos en el controlador de dominio, el grupo UnixAdmins. Tras ello, en las máquinas Linux, en el fichero **/etc/sudoers** añadiremos al final una línea como esta:

```
%unixadmins ALL = (ALL) ALL
```

7. Referencias

Guías PAM

http://www.freebsd.org/doc/en_US.ISO8859-1/articles/pam/
http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/
http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/Linux-PAM_SAG.html

Módulos PAM

http://www.kernel.org/pub/linux/libs/pam/modules.html
http://www.linuxdevcenter.com/pub/a/linux/2001/10/05/PamModules.html

8. Autor

Alfredo Barrainkua Zallo

Iurreta Institutuko Sare Administraria

alfredobz@iurreta-institutua.net