Samba

Última modificación 2009/03

Extraído de "Instalación de Servidor de Dominio y Ficheros":
http://guimi.net/index.php?pag_id=tec-docs/pdc/pdc-instalacion.html

Samba

Contenido

1. CONFIGURACIÓN DE SAMBA

Una gran parte de la información que viene a continuación ha sido extraída de la documentación de Samba.

1.1. INTRODUCCIÓN

a) Posibles problemas con los clientes

Los clientes deben tener instalado el servicio "Cliente de redes Microsoft".
Según indica Microsoft:
"*Windows XP Home Edition no se puede unir a un dominio. Sólo se puede configurar como un miembro de un grupo de trabajo.*"

Para que una maquina con Windows XP Professional pueda acceder al dominio puede ser necesario cambiar la siguiente entrada del registro:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\parameters
```

Y poner "`requiresignorseal`" a 0.
Además en las políticas de seguridad del hay que tener deshabilitadas:

- Miembro de dominio: Descifrar o firmar digitalmente datos de un canal seguro (siempre)
- Miembro de dominio: Deshabilitar cambios de contraseña de cuentas de equipo.
- Miembro de dominio: Requerir clave de sesión protegida (W2000 o más reciente).

b) Configuración del servidor

Una vez configurado el PDC en el servidor a través de Samba dispondremos de:

- Identificación de usuarios
- Gestión de perfiles de usuario
- Ejecución de procesos de conexión (*logon scripts*)

El controlador primario de dominio es un servidor que "gobierna" un dominio de Windows. Lo que hace es centralizar la gestión de usuarios, identificándolos, gestionando sus perfiles y mandándoles procesos a realizar en la conexión.
La identificación de usuarios la realizaremos a través de tdbsam.
Primero se crean los usuarios en Linux, luego se crean en el fichero de samba ('`smbadduser (usuario):(usuario)`') y por último se les incluye en los grupos adecuados para acceder a sus directorios de trabajo. Los usuarios no pueden abrir sesión en el servidor Linux.
Para facilitar la gestión de usuarios utilizamos g-adduser, g-deluser y g-chgpwd.
Los perfiles residen en '`/home/personal/netlogon/profiles/(usuario)`' y se gestionan de forma automática cada vez que un usuario se identifica y siempre que la máquina esté incluida en el dominio del servidor.
Como ya se ha dicho, el proceso de conexión lanza en el cliente un script ('netlogon/scripts/default.bat') cada vez que un usuario se identifica y siempre que la máquina esté incluida en el dominio del servidor.

1.2. INSTALACIÓN

a) Instalamos un servidor DHCP

Si no hay ningún servidor de DHCP en la red instalamos uno:

```
# vi /etc/dhcpd.conf
option domain-name "Mi_Dominio";
option domain-name-servers Servidor.Mi_Dominio;
option subnet-mask 255.255.255.224;
default-lease-time 600;
max-lease-time 7200;

subnet 280.280.280.0 netmask 255.255.255.0 {
    range 280.280.280.100 280.280.280.250;
    option subnet-mask 255.255.255.0;
    option broadcast-address 280.280.280.255;
    option routers 280.280.280.1;
    option domain-name-servers 280.280.280.333;
}
```

b) Instalamos samba

```
# aptitude install samba dhcp samba-common
# vi /etc/samba/smb.conf
# Definiciones globales
[global]
        # Identificacion del equipo
        netbios name = MI_SERVIDOR
        workgroup = MI_DOMINIO
        server string = Servidor %h (Samba %v)
        # Definición de dominio
        security = User
        os level = 64
        domain master = Yes
        local master = Yes
        preferred master = Yes
        domain logons = Yes
        wins support = Yes

        # Gestion de inicio de sesion
        logon script = scripts\default.bat
        logon path = \\%N\profiles\%U #logon path = \\%L\profiles\%U
        logon home = \\%N\%U #logon home = \\%L\%U
        logon drive = H:
        # Caracteristicas de claves
        encrypt passwords = Yes
        obey pam restrictions = Yes
        passdb backend = tdbsam
        # Gestion de claves
        unix password sync = yes
        passwd program = /usr/bin/passwd %u
        passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:*
%n\n *password\supdated\ssuccessfully* .

        # Scripts de gestion de usuarios y equipos
        add user script = /usr/sbin/useradd -m %u
        delete user script = /usr/sbin/userdel -r %u
        add group script = /usr/sbin/groupadd %g
        delete group script = /usr/sbin/groupdel %g
        add user to group script = /usr/sbin/groupmod -A %u %g
        delete user from group script = /usr/sbin/groupmod -R %u %g
        add machine script = /usr/sbin/useradd -s /bin/false -d /var/lib/nobody %u
        # IDs de usuarios y equipos
        idmap uid = 15000-20000
        idmap gid = 15000-20000

        # Registro de sucesos
        log level = 2
        log file = /var/log/samba/log.%m
        max log size = 1000

        # Características extra
        time server = Yes
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        hide dot files = Yes
```

```
# Compartimos los directorios personales
[homes]
        comment = Directorio personal
        path = /home/personal/%S
        valid users = %S
        read only = No
        create mask = 0664
        directory mask = 0775
        browseable = No

# Compartimos el recurso de inicio en red
[netlogon]
        comment = Network Logon Service
        path = /home/personal/netlogon
        read only = Yes
        write list = root
        browseable = No
        guest ok = Yes

# Recurso para los perfiles en red
[profiles]
        comment = Users profiles
        path = /home/personal/netlogon/profiles
        read only = No
        create mask = 0600
        directory mask = 0700
        browseable = No

# Recurso de acceso solo-lectura publico
[publico]
        comment = Directorio publico
        path = /home/trabajo/publico
        guest ok = Yes
        locking = No

# Recursos específicos para grupos
[grupo1]
        comment = Grupo1
        path = /home/trabajo/grupo1
        read only = No
        force create mode = 0660
        force directory mode = 0660

[grupo2]
        comment = Grupo2
        path = /home/trabajo/grupo2
        read only = No
        force create mode = 0660
        force directory mode = 0660
```

c) Creamos los grupos en el servidor:

```
# vi /etc/group
(...)
winusers:x:200:
winsystem:x:201:
winadmin:x:202:
grupo1:x:1001:
grupo2:x:1002:
```

d) Generamos grupos de dominio:

```
# net groupmap add ntgroup="Domain Admins" unixgroup=winadmin rid=512 type=d
# net groupmap add ntgroup="Domain Users" unixgroup=winusers rid=513 type=d
# net groupmap add ntgroup="Domain Guests" unixgroup=nobody rid=514 type=d
```

En caso de no existir el grupo "nobody":

```
# addgroup winguests
# net groupmap add ntgroup="Domain Guests" unixgroup=winguests rid=514 type=d
```

e) Comprobamos los grupos del dominio:

```
# net groupmap list
Domain Users (S-1-5-21-768533834-2550023333-2928700493-1001) -> winusers
Domain Admins (S-1-5-21-768533834-2550023333-2928700493-1005) -> winadmin
Domain Guests (S-1-5-21-768533834-2550023333-2928700493-1006) -> winguests
```

Tomamos nota del identificador del servidor samba (768533834-2550023333-2928700493).
También se puede obtener mediante el comando:

```
# net getlocalsid
```

En caso de cambiar el nombre del servidor Samba se cambiará el SID, con lo que los clientes no podrán validarse.
Al cambiar el nombre del servidor habría que sacar a los clientes del dominio y volverlos a introducir.
Una mejor opción es volver a poner el mismo SID que tenía el servidor antes del cambio de nombre:

```
# net getlocalsid 'OLDNAME'
# net setlocalsid 'SID'
```

f) Garantizamos permisos a "Domain Admins":

```
# net rpc rights grant 'DOMAIN\Domain Admins' (Privilege) -S server -U domadmin
```

Tabla de Privilegios, copiada de la documentación de Samba

Privilege	Description
SeMachineAccountPrivilege	Add machines to domain
SePrintOperatorPrivilege	Manage printers
SeAddUsersPrivilege	Add users and groups to the domain
SeRemoteShutdownPrivilege	Force shutdown from a remote system
SeDiskOperatorPrivilege	Manage disk share
SeTakeOwnershipPrivilege	Take ownership of files or other objects

Para ver los permisos asignados utilizamos el comando:

```
# net rpc list
```

Las principales herramientas para gestionar el servidor son `smbpasswd`, `net` y `pdbedit`.
`smbpasswd` está en proceso de obsolescencia, en su lugar `pdbedit` permite gestionar y consultar usuarios, grupos y políticas de cuentas y accesos.

g) Definición de recursos

Creamos directorios y asignamos permisos

```
# cd /home/personal/
# mkdir netlogon
# chmod 770 netlogon/
# cd netlogon/
# mkdir profiles
# mkdir scripts
# chmod 770 profiles/
# chown winuser:winusers profiles/
# chmod 555 scripts/
# cd scripts/
# wget http://guimi.net/descarga/tec-docs/pdc/default.bat.txt
# ...
```

El directorio '`profiles`' queda en el árbol '`personal`' para que las cuotas controlen su espacio.

Para cumplir las políticas de acceso a los recursos, se ha dado a través de samba acceso a todos los usuarios (identificados). A través del sistema de permisos propio de Linux se ha hecho propietario de cada directorio a '`root`' y a un grupo creado al efecto. En cada directorio solo pueden leer y escribir '`root`' y los usuarios que pertenezcan al grupo, siendo '`root`' el único que puede modificar el directorio en sí.
Al acabar tendremos un árbol similar al siguiente:

```
Directorio         Permisos    Propietario
-------------------------------------------------
/home/
  |- personal          755      root:root
    |- (usuarios)     2770      root:(usuario)
    |-netlogon         770      root:root
      |- profiles      770      root:winusers
        |- (usuarios)  700      root:root
      |- scripts       555      root:root
  |- trabajo           755      root:root
    |- publico        2770      root:winusers
    |- temporal       2770      root:winusers
    |- grupo1         2770      root:grupo1
    |- grupo2         2770      root:grupo2
```