
# Curso avanzado de Linux
# SAMBA

Rafael Varela Pet

Unidad de Sistemas
Área de Tecnologías de la Información y Comunicaciones
Universidad de Santiago de Compostela

# SAMBA

- Paquete Open Source que permite a los sistemas UNIX comunicarse mediante SMB/CIFS
  - SMB = *Server Message Block*
  - CIFS = *Common Internet FileSystem*
- Compartición de archivos e impresoras
- Funcionamiento como cliente y/o servidor

# SAMBA. Nomenclatura

- NetBEUI: Protocolo de transporte. Actúa al mismo nivel que TCP/IP. No empleado por SAMBA
- NetBIOS: API para operaciones en red
- NBT: NetBIOS sobre TCP/IP
- SMB/CIFS funciona sobre NetBIOS en sistemas Windows
- SAMBA es una implementación de NBT y SMB/CIFS

# Servicios

- Servicios presentes en NBT:
  - Servicio de nombres: permite que los equipos se puedan localizar por sus nombres
  - Servicio de datagramas: intercambio de datos en modo desconexión (se usan paquetes UDP)
  - Servicio de sesión: intercambio de datos orientado a conexión (se usa TCP). Es el servicio usado para intercambio de ficheros

# Demonios y utilidades

- Demonios
  - smbd: hace prácticamente todo el trabajo ya que es el que maneja la compartición de archivos e impresoras
  - nmbd: incorpora el servicio de nombres
- Utilidades
  - smbclient
  - nmblookup: permite encontrar nombres NetBIOS en una red, buscar sus dir. IP (entre otras cosas)
  - SWAT (*Samba Web Administration Tool*)

# Puertos

- Puertos empleados en NBT:
  - 137/udp: servicio de nombres
  - 138/udp: servicio de datagramas
- Servicio de sesión:
  - 139/tcp: modo clásico a través de NetBIOS
  - 445/tcp: SMB/CIFS directamente por TCP/IP sin usar NetBIOS

# Instalación en Debian

- Paquetes
  - samba: servidores
  - smbclient: herramientas cliente
  - samba-common: componentes comunes a la parte de servidor y la de cliente

# Resolución de nombres

- Broadcast en la red local
- WINS: Windows Internet Name Service. Servicio semejante al DNS
- Fichero lmhosts: equivalente al fichero hosts de UNIX
- DNS: Método preferido en Windows 2000 en adelante

# Problemática en compartición de archivos

- Mayúsculas/minúsculas
  - UNIX es sensible a mayúsculas
  - Windows “retiene” las mayúsculas
  - DOS solo trabaja en mayúsculas
- Juego de caracteres
- Longitud máxima de los nombres de fichero
- Propietario de los ficheros
- Permisos de acceso /ACLs

# Problemas en la autentificación

- Los sistemas Windows antiguos enviaban las claves en claro => podemos calcular el hash y comparar con lo que tenemos en /etc/shadow
- Actualmente las claves se envían cifradas con un sistema incompatible con el de UNIX.
- Las soluciones:
  - mantener una base de datos separada
  - delegar la autentificación a otra máquina

# Bases de datos de usuarios

- Parámetro passdb backend
  - tdbsam: Trivial Database (TDB)
  - ldapsam
  - nisplussam
  - mysql
- Por defecto, en Debian se utiliza tdbsam
- Ejemplos:

```
passdb backend =
   tdbsam:/etc/samba/passdb.tdbpassdb
passdb backend=ldapsam:ldap://localhost
```

# tdbsam

- Bases de datos en /var/lib/samba. Ejemplos: secrets.tdb, passdb.tdb
- **tdbbackup** permite
  - hacer copias de seguridad
    > `tdbbackup *.tdb`
  - verificar la integridad de la base de datos
    > `tdbbackup -v *.tdb`
- Si instalamos el paquete tdb-tools podemos emplear **tdbtool** y **tdbdump**

# SAMBA. Fichero smbpasswd

- passdb backend = smbpasswd guest
- En /etc/samba/smbpasswd
  - Formato:
    username:uid:HASH LANMAN:HASH NT:Flags:Fecha de modificación
  - Flags:
    U: Usuario normal
    N: Usuario sin clave
    D: Cuenta desactivada
    W: Cuenta de estación de trabajo
  - Ejemplo: [U ]

# Gestión usuarios

- Añadir un usuario

```
> smbpasswd -a nombre_usuario
```

- Cambiar la contraseña a un usuario

```
> smbpasswd nombre_usuario
```

- Habilitar/Deshabilitar un usuario

```
> smbpasswd -e nombre_usuario
> smbpasswd -d nombre_usuario
```

- Borrar un usuario

```
> smbpasswd -x nombre_usuario
```

# SAMBA. Configuración

- En /etc/samba/smb.conf
- Tres bloques:
  - Global
  - Compartición de ficheros
  - Compartición de impresoras
- Secciones especiales:
  [global] [homes] [printers]
- Podemos comprobar nuestra configuración con el comando **testparm**.

# SAMBA. Configuración

- Identificación de nuestra máquina

```
workgroup =
netbios name =
netbios aliases =
```

- Alias: Podemos usar ficheros específicos para cada alias:

```
include = %L.conf
```

- Elección del *master browser.*

```
os level =
local master =
preferred master =
```

# Autentificación

- Encriptación passwords

```
encrypt passwords = yes
```

- Métodos de autentificación (parámetro **security**)
  - share: no hay usuarios. Se asignan contraseñas a los recursos
  - user: se necesita un usuario UNIX en el servidor
  - server: se le reenvía la petición de autentificación a otra máquina.
  - domain: el servidor SAMBA pertenece a un dominio
  - ads: el servidor pertenece a un dominio de Directorio Activo

# Autentificación “server”

- Delega la autenticación en un servidor determinado
- En smb.conf

```
security=server
encrypt passwords = yes
password server =”nombre_servidor”
```

- Se requiere una cuenta UNIX local (puede estar bloqueada)

# Autentificación “domain”

- En smb.conf

```
security=domain
encrypt passwords = yes
workgroup = “nombre_grupo”
password server = *
```

- La máquina tiene que estar registrada en el dominio:

```
> net rpc join -U administrador
```

- Tienen que existir cuentas UNIX locales

# Gestión de cuentas

- Automatizar creación de cuentas UNIX:
  - Usar parámetro add user script:
    - Crea cuentas cuando un usuario se autentifica correctamente
    - Las bajas son manuales
    - Ejemplo
      ```
      add user script = /usr/sbin/useradd %u
      ```
  - **Winbind**: altas y bajas dinámicas. El equipo es un miembro completo del dominio

# SAMBA. Winbind

- Winbind permite:
  - Verificar las credenciales de un usuario (vía PAM).
  - Resolución de la identidad (vía NSS).
  - Winbind mantiene una base de datos independiente (winbind_idmap.tdb) en la que se almacena la asociación entre UIDs / GIDs UNIX y los SIDs de NT.
- Requisitos previos:
  - Nuestro servidor debe estar unido al dominio
  - Instalamos paquete **winbind**

# Winbind. Configuración

- Editar smb.conf:

```
security = domain

winbind use default domain = yes
winbind separator = +
winbind cache time = 300

idmap uid = 10000-20000
idmap gid = 10000-20000

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

winbind enum groups = yes
winbind enum users = yes
```

# Winbind. Configuración

- En caso de tener muchos usuarios, puede considerarse:

```
winbind enum groups = no
winbind enum users = no
```

  - Pero puede provocar problemas a ciertas aplicaciones
- Ajustar el parámetro “valid users” en la sección [homes]

```
valid users = %S
```

# Winbind. Configuración

- Parámetro "**winbind separator**":
  - Define el carácter empleado cuando se muestra un usuario en la forma DOMINIO\usuario.
  - Sólo se aplica cuando usamos los módulos pam_winbind.so y nss_winbind.so para los servicios UNIX
  - Algunos caracteres problemáticos
    - \+ : También se emplea con NIS en /etc/group
    - \\ : Carácter de escape en el shell

# Winbind. Configuración

- Con Windows Server 2003
  - Editar sección [global] de smb.conf

    ```
    client schannel = no
    ```

  - Asignar usuario para establecer sesión con un controlador de dominio. Ejecutar:

    ```
    > wbinfo –set-auth-user=usuario%clave
    ```

- Alternativa. Emplear Kerberos.
  - En smb.conf:

    ```
    security=ads
    ```

# Winbind. Pruebas

- Unirnos al dominio e iniciar winbind
- Probar configuración:
  - `> wbinfo -p` (hace 'ping')
  - `> wbinfo -t`
    (comprueba la cuenta de la máquina en el dominio)
  - `> wbinfo -g` (lista grupos)
  - `> wbinfo -u` (lista usuarios)
- El *resolver* UNIX tiene que encontrar la información en DNS del Servidor de Dominio.
  - Ajustar contenido de /etc/resolv.conf

# Winbind. NSS.

- NSS (*Name Service Switch*): sistema modular para acceder a las bases de datos usadas por la librería C.
- Configurar NSS
  - Editar /etc/nsswitch.conf

```
passwd: files winbind
group: files winbind
```

- Probar NSS:

```
> getent group
> getent passwd
```

# Winbind. PAM

- Podemos autenticar otros servicios vía PAM
- Editar el fichero /etc/pam.d correspondiente al servicio que queremos modificar
- Ejemplo: OpenSSH, editar /etc/pam.d/ssh:

```
auth sufficient pam_winbind.so
@include common-auth
...
account    sufficient   pam_winbind.so
@include common-account
...
```

- Conectar al servidor SSH:

```
> ssh DOMINIO+usuario@servidor_ssh
```

# Winbind y Kerberos

- El método anterior es compatible con dominios pre-windows 2000
- Con Directorio Activo podemos emplear Kerberos
- En smb.conf:

```
realm = CURSOLINUX.LOCAL
security = ADS
encrypt paswords = yes
password server = servidor_kerberos
```

(esto último, sólo si no es capaz de localizarlo)

# Winbind. Kerberos

- Instalar krb5-user, krb5-clients  y krb5-config
- /etc/krb5.conf

```
[libdefaults]
   default_realm = CURSOLINUX.LOCAL
[realms]
   CURSOLINUX.LOCAL = {
         kdc = 192.168.253.21
         admin_server = 192.168.253.21
   }
[domain_realm]
   .cursolinux.local = CURSOLINUX.LOCAL
   cursolinux.local = CURSOLINUX.LOCAL
```

# Winbind. Kerberos

- Sincronizar reloj del equipo Debian

```
> net time set
```

- Probar kerberos:

```
> kinit usuario@CURSOLINUX.LOCAL
> klist
```

- Unirse al dominio y almacenar la cuenta del equipo en la unidad organizativa “computers”:

```
> kinit administrador@CURSOLINUX.LOCAL
> net ads join createcomputer="Computers"

Using short domain name -- CURSOLINUX
Joined 'DEBIAN' to realm 'CURSOLINUX.LOCAL'
```

# Winbind. Directorio Activo

- Probar Winbind:

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

> wbinfo -p
Ping to winbindd succeeded on fd 4

> wbinfo -t
checking the trust secret via RPC calls
succeeded

> wbinfo -g
> wbinfo -u
```

# Winbind. Directorio Activo

- Pruebas desde clientes Windows

```
> net use * //servidorSamba/share
```

- smbclient: Emplear la opción -k para autenticación Kerberos:

```
> smbclient -k //servidor/share
```

# Resolución de problemas

- Comprobar desfase horario entre los relojes del controlador de dominio y de los clientes
- Revisar resolución de nombres:
  - Dominio DNS y *realm* Kerberos deben coincidir
  - Los nombres FQDN de los equipos deben resolver correctamente
  - Debe coincidir el nombre UNIX (/etc/hosts) y el nombre NetBIOS en smb.conf
  - Comprobar salida del comando “hostname --fqdn”

# Referencias

- www.samba.org
- http://us1.samba.org/samba/docs/man/Samba-Guide/
- http://samba.org/samba/docs/man/Samba-HOWTO-Collectior
- http://web.mit.edu/kerberos/www/