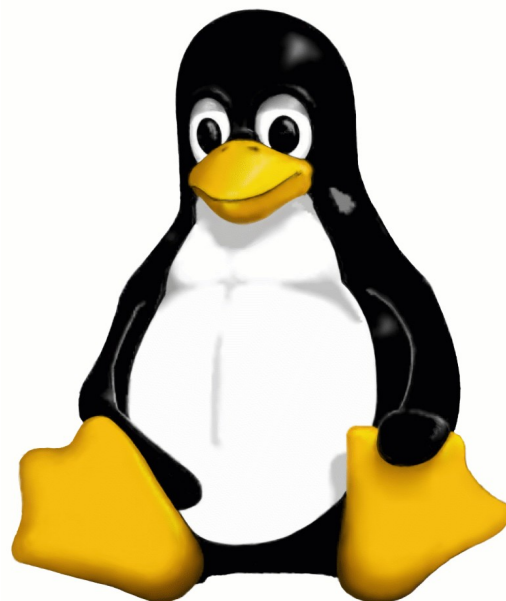


# CURSO LINUX: Administración de Sistema y Servicios

(parte 4)



### Samba

- Implementación GPL de NetBIOS y SMB.
- Servicios que ofrece Samba:
  - Servicios de acceso remoto a ficheros e impresoras.
  - Autenticación y autorización.
  - Resolución de nombres.
  - Anuncio de servicios.
- Versión actual: 3

### Partes de Samba

- Samba consta de dos programas:
  - smb
  - nmb

### smbd

- Ofrecer acceso remoto a ficheros e impresoras (implementando el protocolo SMB).
- Autenticar y autorizar usuarios.
- 2 modos de compartición de recursos:
  - ➔ Basado en usuarios (Windows NT ó 2000): Acceso basado en usuario/password en un dominio.
  - ➔ Basado en recurso (Windows 3.11 ó 95): Acceso basado en recurso/password.

nmbd

- El sistema Unix participa en los mecanismos de resolución de nombres propios de Windows:
  - Anuncio en grupo de trabajo.
  - Listado de ordenadores del grupo de trabajo.
  - Anuncio de recursos compartidos.
- ¡ El sistema Unix aparece en el “Entorno de red” !

## SMB

- Protocolo de comunicación de alto nivel que puede implementarse sobre diversos protocolos:
  - TCP/IP
  - NetBEUI
  - IPX/SPX
- Se implementa habitualmente encima de NetBIOS sobre TCP/IP.
- Desarrollado inicialmente por IBM como el IBM PC Network SMB Protocol o Core Protocol a principios de los años 80.
- Diferentes añadidos de fabricantes (Microsoft).

## SBM (II)

- Ejemplo de funcionamiento: un cliente desea acceder a carpeta compartida de un servidor (modo “user”):

**Petición: Sesión NetBIOS.**

**Respuesta: Sesión NetBIOS (ACK).**

**Petición: Dialecto SMB (versiones Samba que soporta el cliente).**

**Respuesta: Dialecto SMB.**

**Petición: Inicio de sesión, envío de usuario/dominio/password.**

**Respuesta: Inicio de sesión. Comprueba autenticación y luego autorización.**

**Petición: Conexión a un recurso concreto. ([\\pc01\carpeta](#))**

**Respuesta: Conexión a un recurso concreto.**

### Instalación en Debian

- Instalar el paquete Samba:
  - ```
#> apt-get install samba
```
  - Nos pregunta si queremos “copiar” todos los usuarios existentes de sistema a cuentas Samba.
    - ¡ Ojo, no atiende a futuros cambios de password ni adición/eliminación/modificación de usuarios !
- Datos en `/etc/samba/` y `/var/lib/samba/`.

## Configuración Samba

- Fichero `/etc/samba/sbm.conf`
  - [global]
    - Parámetros blogales y parámetros por defecto en el resto de las secciones.
  - [homes]
    - Define automáticamente un recurso de red por cada usuario conocido por Samba. Este recurso, por defecto, está asociado al directorio de conexión de cada usuario en el ordenador en el que Samba está instalado.
  - [printers]
    - Define un recurso compartido por cada nombre de impresora conocida por Samba.
  - [otro\_recurso\_1]
  - [otro\_recurso\_2]

[global]

| Opción            | Significado                                                                                                                                                                                      | Valor por defecto                                       |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| netbios name      | Nombre (NetBIOS) del ordenador Samba.                                                                                                                                                            | Primer componente del nombre DNS del ordenador.         |
| workgroup         | Nombre del dominio (o grupo de trabajo) al que pertenece Samba.                                                                                                                                  | nulo                                                    |
| security          | Nivel de seguridad (share, user, server, domain).                                                                                                                                                | user                                                    |
| encrypt passwords | Utilizar contraseñas cifradas de Windows (en modo domain, sí deben utilizarse).                                                                                                                  | no                                                      |
| password server   | Ordenador Windows utilizado para la autenticación. En modo domain, debe ser una lista de los DCs del dominio.                                                                                    | nulo                                                    |
| map to guest      | Establece en qué condiciones un acceso a Samba debe considerarse en modo invitado (en el nivel domain, este parámetro afecta sólo cuando el acceso no ha sido acreditado por el DC del dominio). | never                                                   |
| log level         | Nivel de detalle en la auditoría de Samba. Es un número que indica la cantidad de información a auditar. A mayor valor, más cantidad de información.                                             | Se establece en el script que inicia el servicio Samba. |
| log file          | Nombre del fichero donde se almacenan mensajes de auditoría de Samba.                                                                                                                            | Se establece en el script que inicia el servicio Samba. |

### [nombre\_recurso]

| Opción                            | Significado                                                                                                                   | Valor por defecto                                                             |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| read only<br>({yes/no})           | Recurso exportado como sólo lectura.                                                                                          | yes                                                                           |
| browseable<br>({yes/no})          | El servicio aparece en la lista de recursos compartidos al explorar el ordenador Samba desde el Entorno de Red Windows.       | yes                                                                           |
| path                              | Ruta absoluta al directorio compartido por el recurso.                                                                        | nulo                                                                          |
| comment                           | Descripción del servicio (cadena de caracteres).                                                                              | nulo                                                                          |
| guest ok<br>({yes/no})            | Permitir accesos como invitado al recurso.                                                                                    | no                                                                            |
| guest account                     | Si un acceso se realiza como invitado, se utiliza el usuario indicado para representar la conexión.                           | nobody                                                                        |
| guest only<br>({yes/no})          | Todos los accesos se aceptan en modo invitado.                                                                                | no                                                                            |
| copy                              | Duplica otro recurso existente.                                                                                               | nulo                                                                          |
| force user                        | Los accesos al recurso se realizan como si el usuario que accede es el usuario indicado.                                      | nulo (se utiliza el mismo usuario que ha realizado la conexión).              |
| force group                       | Los accesos al recurso se realizan como si el usuario que accede pertenece al grupo indicado.                                 | nulo (se utiliza el grupo primario del usuario que ha realizado la conexión). |
| hosts allow                       | Lista ordenadores desde los que se permite acceder al recurso                                                                 | lista vacía (i.e., todos los ordenadores).                                    |
| hosts deny                        | Lista ordenadores desde los que no se permite acceder al recurso. En caso de conflicto, prevalece lo indicado en hosts allow. | lista vacía (ningún ordenador).                                               |
| valid users                       | Lista de usuarios que pueden acceder al recurso.                                                                              | lista vacía (i.e., todos los usuarios).                                       |
| follow symlinks<br>({yes/no})     | Permitir el seguimiento de los enlaces simbólicos que contenga el recurso.                                                    | yes.                                                                          |
| inherit permissions<br>({yes/no}) | Al crear ficheros y subdirectorios nuevos, estos heredan los permisos Unix de la carpeta donde se crean.                      | no.                                                                           |

## Algunos comandos

- testparm: Comprueba la configuración del smb.conf y nos avisa de errores y avisos.
- smbpasswd: Administración de usuarios Samba:

Creación de un usuario:

```
#> smbpasswd -a usuario
```

Modificación de password de un usuario:

```
#> smbpasswd usuario
```

Más: ;)

```
#> smbpasswd -help
```

- smbclient: Cliente Samba en consola:

```
#> smbclient -L netbios_name
```

```
#> smbclient -I IP (para forzar el servidor)
```

```
#> smbclient -U usuario -L netbios_name
```

## Montar un recurso Samba

- Requiere el paquete “smbfs”:

```
#> apt-get install smbfs
```

- Requiere cargar el módulo “smbfs”:

```
#> modprobe smbfs
```

- Sintaxis:

```
#> mount -t smbfs -o username=XX,password=XX,workgroup=XX  
//ip_servidor/nombre_recurso /punto_montaje
```

- O en el /etc/fstab:

```
//ip_servidor/nombre_recurso /punto_montaje smbfs username=XX,password=XX
```

## OpenLDAP

- Implementación libre del protocolo LDAP (Lightweight Directory Access Protocol).
- Plataformas soportadas:  
`Linux, BSD, AIX, HP-UX, Mac OSX, Solaris, Microsoft Windows (2000, XP)`

### Componentes de OpenLDAP

- slapd: Demonio LDAP que atiende a las consultas.
- slurpd: Demonio de replicación.
- Utilidades y herramientas (línea de comandos).

### Características

- Versión actual: 2.X
  - Múltiples bases de datos
  - Múltiples backends de almacenamiento
  - Soporte LDAP v3
  - IPv6
  - Simple Authentication and Security Layer ([SASL](#))

### Instalación en Debian Sarge

```
#> apt-get install slapd
```

- Debconf nos pregunta:

- Dominio raíz:

```
dominio.org -> dc=dominio,dc=org
```

- Password de administrador:

```
Password del usuario cd=admin,dc=dominio,dc=org
```

- Backend de almacenamiento:

```
BDB
```

- Iniciar/parar/reiniciar el servicio:

```
#> /etc/init.d/slapd start/stop/restart
```

- Reconfigurar slapd:

```
#> dpkg-reconfigure slapd
```

- ¡ Borramos la base de datos y la configuración !

### Fichero /etc/ldap/slapd.conf

```
# No permitimos protocolo LDAP v2:
#allow bind_v2

# Esquemas incluidos:
include          /etc/ldap/schema/core.schema
include          /etc/ldap/schema/cosine.schema
include          /etc/ldap/schema/nis.schema
include          /etc/ldap/schema/inetorgperson.schema

[...] Datos necesarios. Valores por defecto.
```

## Fichero /etc/ldap/slapd.conf (II)

```
# Definición de una base de datos (comienza con "database"):  
database          bdb  
  
suffix            "dc=dominio,dc=org"  
directory         "/var/lib/ldap"  
  
# Usuario administrador: ¡OJO! Debian no lo usa, emplea ACL's en  
# su lugar:  
#rootdn "cn=root,dc=dominio,dc=org"  
# El password lo podemos poner en claro o cifrado (usamos el  
# comando "slappasswd" para generar un password cifrado y lo  
# copiamos aquí:  
#rootpw {SSHA}Ok++H+ZzR4UYkHxbtoL9ZRCcPvtxcJu0
```

- Recordad que en Debian por defecto NO se usa la cuenta "rootdn" sino ACL's (ver siguiente transparencia)

## Fichero /etc/ldap/slapd.conf (III)

```
# ACL's: el usuario definido "admin" tiene todos los
# permisos gracias a ACL's, pero sigue siendo una entrada dentro
# del LDAP:

# Cada usuario puede cambiar su password,
# todos pueden autenticarse,
# "admin" puede cambiar cada password:
access to attrs=userPassword
    by dn="cn=admin,dc=dominio,dc=org" write
    by anonymous auth
    by self write
    by * none

# Permitimos lectura de todo el árbol a usuarios anónimos
# (necesario para permitir mecanismos de autenticación):
access to dn.base="" by * read

# "admin" tiene acceso de escritura a todo:
access to *
    by dn="cn=admin,dc=alix,dc=net" write
    by * read
```



## ACL's

- Se definen en el “database” en /etc/ldap/slapd.conf
- La primera ACL que coincida es la que se aplica.
  - ¡ Primero las ACL's más restrictivas !
- Explicación detallada y ejemplos:
  - <http://www.openldap.org/doc/admin22/slapdconfig.html#Access%20Control>
  - <http://es.tldp.org/COMO-INSFLUG/COMOs/LDAP-Linux-Como/LDAP-Linux-Como-3.html#ss3.5>

### Esquemas

- Se guardan en `/etc/ldap/schema`
- Para habilitar cada esquema:
  - `/etc/ldap/slapd.conf`:
- Algunas aplicaciones proveen de su propio esquema.
  - Ejemplo: Samba ofrece su “`samba.schema`” en el paquete “`samba-doc`”:

```
include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
...
```

```
/usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz
```

- Descomprimirlo con “`gzip -d samba.schema.gz`”.
- Copiarlo a `/etc/ldap/schema`
- Habilitarlo en `/etc/ldap/slapd.conf`:

```
include      /etc/ldap/schema/samba.schema
```

### phpLDAPadmin

phpLDAPadmin - 0.9.8.3

- Home
- Request feature
- Donate
- Purge caches
- Report a bug
- Help

**My LDAP Server**

( [schema](#) | [search](#) | [refresh](#) | [info](#) | [import](#) | [export](#) | [logout](#) )

Logged in as: cn=admin

- dc=aliax,dc=net (6)
  - cn=admin
  - ou=dns (1)
  - ou=hosts (1)
    - dc=aliax.net (1)
      - dc=ibc
      - ★ Create new entry here
    - ★ Create new entry here
  - ou=sugarcrm (3)
  - ou=Users (1)
    - uid=ibc\_ldap
    - ★ Create new entry here
  - uid=maquina1
  - ★ Create new entry here

dc=ibc

Server: **My LDAP Server** Distinguished Name: **dc=ibc,dc=aliax.net,ou=hosts,dc=aliax,dc=net**

- Refresh
- Copy or move this entry
- Delete this entry
- Hint: To delete an attribute, empty the text field and click save.
- Compare with another entry
- ★ Create a child entry
- Hint: To view the schema for an attribute, click the attribute name.
- Export
- Show internal attributes
- Rename
- Add new attribute

**aRecord**

(add value)

**associatedDomain**

ibc.aliax.net  
(add value)

**dc** RE

ibc  
(rename)

**hInfoRecord**



## phpLDAPAdmin (II)

- Instalación en Debian:

```
#> apt-get install phpldapadmin
```

- Crea un "Alias" en /etc/apache2/conf.d:

```
Alias /phpldapadmin /usr/share/phpldapadmin
```

- Acceso web:

- URL:

```
http://IP/phpldapadmin
```

- Usuario:

```
cn=admin,dc=dominio,dc=org
```



## Servidor DNS PowerDNS

- Servidor DNS bajo GPL.
- Plataformas \*nix y Windows.
- Distintos backends para almacenar las zonas:  
`bind, db2, gmysql, gpsql, goracle, gsqlite, ldap, odbc, opendbx, pipe`
- Características:
  - Transferencia de zonas
  - Caché
  - Notificación de cambios
  - Modo chroot
  - Monitorización vía web

### Instalación en Debian

- Vamos a usar el backend LDAP:

```
#> apt-get install pdns-server pdns-backend-ldap
```

→ Se crea el fichero /etc/ldap/schema/dnsdomain2.schema.

- Clase dNSDomain2: Incluye atributos para registros SRV, A6Record, PTR...

→ Lo habilitamos en slapd.conf.

- Manejar el servicio:

```
/etc/init.d/pdns start|stop|restart|monitor
```



## /etc/powerdns/pdns.conf

```
# Opciones interesantes (el resto por defecto):

# launch: tipo de backend.
launch=ldap
ldap-host=127.0.0.1:389
ldap-basedn=ou=hosts,dc=dominio,dc=org
# Tipo de búsqueda (más adelante):
ldap-method=strict

# disable-axfr: Deshabilita (o no) las transferencias de zonas,
# es decir, el hacer un "host -l dominio".
disable-axfr=no

# allow-axfr-ips: Si "disable-axfr=yes" se permite transferencia de
zonas a estas IP's o rangos:
#allow-axfr-ips=

# cache-ttl: Segundos de cacheo en el PacketCache:
# http://doc.powerdns.com/performance-settings.html#PACKETCACHE
cache-ttl=20
```

### /etc/powerdns/pdns.conf (II)

```
# recursor: IP del servidor DNS externo:  
recursor=80.58.0.33
```

```
# allow-recursion: IP's o rangos (separados por comas) pueden pedir  
# recursión, es decir, que PowerDNS consulte al DNS externo  
# (parámetro "recursor"):  
allow-recursion=127.0.0.1,192.168.1.1/24
```

## ldap-method

- tree
  - La opción más rápida para encontrar las consultas.
  - Se representa en LDAP el árbol completo del dominio.

```
dc=dominio,dc=org
+ ou=hosts (ldap-basedn=ou=hosts,dc=dominio,dc=org)
+ dc=org
  + dc=dominio (registros SOA, NS, MX...)
  + dc=www
  + dc=ftp
```

## Idap-method (II)

- simple
  - No se necesita orden jerárquico (es opcional).
  - Se utiliza el atributo “associatedDomain”:

```
dn: dc=dominio.org,ou=hosts,dc=dominio,dc=org
associatedDomain: dominio.org
dc: dominio.org
nSRecord: ibc
objectClass: dcObject
objectClass: dNSDomain2
objectClass: domainRelatedObject
objectClass: top
sOARRecord: ibc.dominio.org ibc@dominio.org 2 1801 3601 86401 7201
```

```
dn: dc=ibc,dc=dominio.org,ou=hosts,dc=dominio,dc=org
associatedDomain: ibc.dominio.org
dc: ibc
aRecord: 90.90.90.90
hInfoRecord: Kubuntu Edgy
objectClass: dcObject
objectClass: dNSDomain2
objectClass: domainRelatedObject
objectClass: top
```

### Idap-method (III)

- strict
  - Igual que “simple”.
  - Pero añade automáticamente resolución inversa.

```
#> host -t ptr IP
```

## Paquetes útiles para Debian Sarge

- modconf:
  - Menú gráfico para cargar/descargar módulos.
  - Incluye los módulos en /etc/modules.
    - ¡ Se cargarán en el próximo arranque !
- rcconf:
  - Menú gráfico para activar/desactivar servicios en el arranque.
- vim:
  - Vi mejorado (más sencillo de usar).
  - /etc/vim/vimrc:

```
syntax on      (activar colores)
set background=dark  (consola fondo oscuro)
"set autoindent  (no activar, da problemas con el ratón)
"set linebreak   (no cortar palabras al pasar de línea)
set ignorecase   (en búsquedas no importa mayúscula/mínuscula)
```

## Recuperar Grub o password de root

- Arrancar con liveCD (Knopix, (K)Ubuntu...).
- Montar **manualmente** la partición / del disco duro:
  - `#> mount -t ext3 /dev/hdaX /mnt/hdaX`
    - ¡Ojo! /mnt/hdaX debe existir (sino se crea antes)
- Nos hacemos root en el Linux del disco duro (hdaX):
  - `#> chroot /mnt/hdaX`
    - ¡Ahora los comandos y configuración son las del disco!
- Recuperar Grub:
  - Modificar (si hace falta) /boot/grub/menu.lst
  - Escribir en el MBR del disco duro:
    - `#> grub-install /dev/hda`
      - ¡Ojo, no se pone la partición "hdaX" sino el disco primario "hda"!
- Reiniciar y ya está ;)

### Recuperar Grub o password de root (II)

- Cambiar password de root (es imposible averiguarlo):
  - `#> passwd`
    - Al ser root no nos pedirá el password anterior.
- Reiniciar y ya está ;)

