

Cheat-Sheet: Samba4 Debian GNU/Linux

Samba4: Integra DNS, LDAP e Kerberos Heimdal AD DC (Active Directory Domain Controller)

Cheat Sheet Samba4
ESCENARIO Server Standalone
Rede: 172.16.10.0/24 GW: 172.16.10.1
DNS1: 8.8.4.4 DNS2: 8.8.8.8
A: 172.16.10.254/24 B: 172.16.10.150/24
Debian 64bits Debian 64bits
NTP, SAMBA4Hostname: lclient1
(DNS,LDAP,KERBEROS) Servidor SSH
Hostname: lserver1
Servidor SSH
sda: SO instalado
sd[bcd]: array de discos

C: 172.16.10.2/24
Debian 64bits + XFCE
Cliente SSH
Hostname: sshclient

root/abc123.
usuario/abc123.



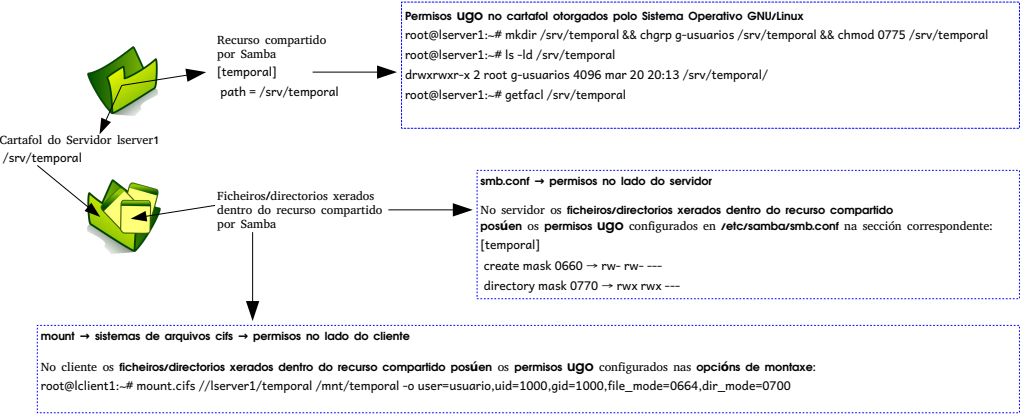
Host Anfitrión → Rede NAT
\$ vboxmanage list natnets
NetworkName: LinuxNatNetwork
IP: 172.16.10.1
Network: 172.16.10.0/24
...
Oracle VM VirtualBox
Rede NAT: 172.16.10.0/24
172.16.10.1 → GW (Router)
172.16.10.2/24 → Host Anfitrión
172.16.10.3/24 → DHCP
[172.16.10.4, 172.16.10.254] → Range DHCP

Prioridade Permisos +

Sistema arquivos Servidor

Configuração Samba

Montaxe no Cliente



SERVIDOR AD-DC	CLIENTE DO DOMINIO
(1) Preparativos NTP, DNS	
(2) Aprovisionamento samba-tool	
(3) Administración AD ldb-tools + LDIF → UO samba-tool → usuarios/grupos	
(4) Listar usuarios/grupos UNIX + LDB nslcd, nscd getent	
(5) Preparativos NTP, DNS → Servidor Samba AD-DC, hostname pbis → Configuración global perfil usuario → Unir/abandonar dominio → Servidor ssh (openssh-server)	
(6) Aprovisionamento domainjoin-cli join/leave	
(7) Verificar acceso usuarios ttyX, ssh	
(8) Recursos Compartidos Arrays de discos	
(9) ACLs mkdir, chgrp, chmod setfacl, getfacl	
(10) Tarefas programadas /etc/crontab → eliminar datos temporais nos recursos compartidos	
(11) Recursos compartidos libpam-mount (sgrp → grupo) ttyX, ssh, su - login → montar logout → desmontar	
(12) Cotas usuario soft, hard quota, quotacheck setquota, edquota	
(13) Scripts Inicio de Sesión /etc/profile → script bash → if grupo	

Ricardo Feijoo Costa



This work is licensed under a **Creative Commons Attribution-ShareAlike 4.0 International License**

Controlador de dominio

Controlador de dominio

(PDC)
(NTP)
(DNS)
(LDAP)
(Kerberos)

NTP (sincronizar hosts para validez de tickets Kerberos)

```
# apt -y install ntp
# A=$(grep -n ^#server /etc/ntp.conf | cut -d':' -f1 | xargs | awk '{print $NF}')
# sed -i "${A}s/server 2.es.pool.ntp.org iburst prefer\nserver 1.europe.pool.ntp.org iburst\nprefer\nserver 2.europe.pool.ntp.org iburst prefer" /etc/ntp.conf
# systemctl restart ntp.service
# ntpq -p
```

→ Cambiar os **servidores ntp** cos que sincronizar o sistema

HOSTNAME FQDN (configurar nome DNS do servidor SAMBA para resolución DNS e reino Kerberos)

```
# echo 'lserver1.ies.local' > /etc/hostname
# sed -i 's/lserver1/lserver1.ies.local lserver1/' /etc/hosts
# echo 'kernel.hostname=lserver1.ies.local' >> /etc/sysctl.conf
# sysctl -p
```

→ Configurar o nome DNS no equipo servidor SAMBA

AD DC (Active Directory Domain Controller) (configurar o Servidor SAMBA como Controlador de Dominio)

```
# dpkg -l bind9 | grep un && [ $? -ne 0 ] && apt -y purge bind9 → Purgar se é o caso o servidor DNS bind9.
# dpkg -l dnsmasq | grep un && [ $? -ne 0 ] && apt -y purge dnsmasq → Purgar se é o caso o servidor DNS/DHCP dnsmasq
```

```
# mv /etc/samba/smb.conf smb.conf.standalone.server
# samba-tool domain provision --use-rfc2307 --realm=IES.LOCAL --domain=IES --server-role=dc \
--dns-backend=SAMBA_INTERNAL --adminpass=abc123.
...
Server Role:          active directory domain controller
Hostname:             lserver1
NetBIOS Domain:       IES
DNS Domain:           ies.local
DOMAIN SID:           S-1-5-21-307976336-692820594-3996066041
```

→ Promocionar a PDC

```
# apt -y install winbind
# systemctl unmask samba-ad-dc
# systemctl stop smbd && systemctl stop nmbd
# systemctl start samba-ad-dc
# systemctl enable samba-ad-dc
```

→ Activar servizo **samba-ad-dc**
(Ver Servizo/s)

```
# echo -e "domain ies.local\nsearch ies.local\nnameserver 172.16.10.254" > /etc/resolv.conf
# host -t SRV ldap.tcp.ies.local.
ldap.tcp.ies.local has SRV record 0 100 389 lserver1.ies.local.
# host -t SRV kerberos.tcp.ies.local.
kerberos.tcp.ies.local has SRV record 0 100 88 lserver1.ies.local.
# host -t A lserver1.ies.local.
lserver1.ies.local has address 172.16.10.254
```

→ DNS: Apuntar ao servidor SAMBA e Verificar a resolución DNS: ldap, kerberos, hostname

Configuración
(/etc/samba/smb.conf)
(testparm)
(man 5 smb.conf)
(man 7 samba)
(man 8 samba)

→ Comentarios (opcións por defecto)
; → Comentarios (opcións que difiren das de por defecto)
[global] → Sección **obligatoria** correspondente á configuración global.
[netlogon] → Sección **obligatoria** correspondente aos scripts que se executan durante o inicio de sesión (login)
[sysvol] → Sección **obligatoria** correspondente aos ficheiros públicos dun dominio que se replican en cada controlador de dominio

[global]

dns forwarder = 8.8.4.4 → DNS ao que enviar peticións cando o DNS Interno de SAMBA non poida resolver
netbios name = LSERVER1 → Nome netbios
realm = IES.LOCAL → Reino Kerberos
server role = active directory domain controller → Modo de operación de samba. Pode tomar valores: "standalone server", "member server", "classic primary domain controller", "classic backup domain controller", "active directory domain controller". Neste caso **controlador de dominio**.
workgroup = IES → Nome do grupo de traballo do equipo
idmap_ldb:use rfc2307 = yes → O uso de atributos RFC 2307 permite o almacenamento de información de grupos e usuarios de Unix nun directorio LDAP.

[netlogon]

path = /var/lib/samba/sysvol/ies.local/scripts → Accédese ao recurso compartido /var/lib/samba/sysvol/ies.local/scripts mediante o nome da sección netlogon.
read only = No → Permisos de escritura

[sysvol]

path = /var/lib/samba/sysvol → Accédese ao recurso compartido /var/lib/samba/sysvol/ mediante o nome da sección sysvol.
read only = No → Permisos de escritura

Servizo/s

(smbd
&&
nmbd)
(man 8 smbd
&&
man 8 nmbd)
(samba-ad-dc
&&
winbind)
(man 8 winbindd)

Servidor Independente: smbd && nmbd

smbd && nmbd → Por defecto cando se instala Samba configúrase como Servidor Independente, enmáscase o servizo samba-ad-dc, e debemos empregar os servizos smbd e nmbd.

systemctl status smbd && systemctl status nmbd → Ver estado
systemctl start smbd && systemctl start nmbd → Arrancar
systemctl stop smbd && systemctl stop nmbd → Parar
systemctl reload smbd && systemctl reload nmbd → Recargar
smbcontrol all reload-config → Recargar

Controlador de dominio: samba-ad-dc

samba-ad-dc → Cando configuramos Samba como AD-DC debemos instalar winbind e desenmascarar o servizo samba-ad-dc para poder empregalo.

apt -y install winbind → Instalar winbind
systemctl status samba-ad-dc → Ver estado
systemctl unmask samba-ad-dc → Desenmascarar
systemctl stop smbd && systemctl stop nmbd → Parar smbd && nmbd
systemctl start samba-ad-dc → Arrancar
systemctl stop samba-ad-dc → Parar
systemctl reload samba-ad-dc → Recargar
systemctl enable samba-ad-dc → Habilitar(/etc/rcX.d)

LDAP (ldb-tools) (ldif)

O paquete `ldb-tools` ofrece unha serie de comandos para a administración de datos no directorio LDAP. Os comandos para engadir, modificar, buscar, eliminar, editar e renomear son respectivamente: `ldbadd`, `ldbmodify`, `ldbsearch`, `ldbdel`, `ldbedit` e `ldbrename`. Permiten ser empregados con arquivos LDIF e posúen unha sintaxe similar aos comandos `openldap`, do paquete `ldap-utils`, equivalentes (`ldapadd`, `ldapmodify`, `ldapsearch`, `ldapdelete` ...).

OU → Unidade Organizativa

`apt -y install ldb-tools`

`ldbmodify -H ldap://localhost -Uadministrator%abc123. create-OU.ldif`

`ldbadd -H ldap://localhost -Uadministrator%abc123. create-OU.ldif`

`ldbsearch -H ldap://localhost -Uadministrator%abc123. OU=ies`

`ldbsearch -H ldap://localhost -Uadministrator%abc123. -b 'OU=ies,DC=ies,DC=local'`

`ldbsearch -H ldap://localhost -Uadministrator%abc123. -b 'ou=IES,DC=iEs,DC=lOcal'`

`ldbmodify -H ldap://localhost -Uadministrator%abc123. delete-OU.ldif`

~~# `ldbdel -H ldap://localhost -Uadministrator%abc123. delete-OU.ldif`~~

→ Instalar

→ Crear OU a través do arquivo `ldif`
`create-OU.ldif`

→ Comando equivalente ao anterior.

Buscar rexistros
→ correspondentes a OU=ies en IES.LOCAL

Buscar rexistros
→ correspondentes a OU co basedn
OU=ies,DC=ies,DC=local en IES.LOCAL

→ Comando equivalente ao anterior.

→ Eliminar OU a través do arquivo
`ldif delete-OU.ldif`

Non podemos executar `ldbdel` en vez de `ldbmodify` xa que o comando `ldbdel` non admite arquivos `ldif` como parámetro/s.

Arquivos LDIF

Nun arquivo LDIF pode haber mais dunha entrada definida. Cada entrada sepárase das demais por unha liña en branco e pode ter unha cantidade arbitraria de pares `<nome_atributo>: <valor>`

create-OU.ldif

```
dn: OU=ies,DC=ies,dc=local
changetype: add
objectClass: top
objectClass: organizationalunit
description: ies OU
```

```
dn: OU=usuarios,OU=ies,DC=ies,dc=local
changetype: add
objectClass: top
objectClass: organizationalunit
description: usuarios OU
```

delete-OU.ldif

```
dn: OU=usuarios,OU=ies,DC=ies,dc=local
changetype: delete
```

```
dn: OU=ies,DC=ies,dc=local
changetype: delete
```

samba-tool

samba-tool → evolución de pdbedit → evolución de smbpasswd

```
# samba-tool group add g-usuarios \
--groupou=OU=USUARIOS,OU=IES --nis-domain=ies --gid-number=10000
```

→ Crear grupo SAMBA g-usuarios

```
# samba-tool user create anxo --random-password --must-change-at-next-login \
--userou='OU=Usuarios,OU=IES' --gecos 'Pertencente a g-usuarios' \
--uid-number=11000 --gid-number=11000 --login-shell=/bin/bash \
--mail-address=anxo.carballeira@ies.local --telephone-number=639111111
```

→ Crear o usuario de forma local

```
# samba-tool user create brais 123passbraisABC --must-change-at-next-login \
--userou='OU=Usuarios,OU=IES' --gecos 'Pertencente a g-usuarios' \
--uid-number=11001 --gid-number=11001 --login-shell=/bin/bash \
--mail-address=brais.peiteado@ies.local --telephone-number=639222222 \
-H ldap://localhost -Uadministrator%abc123.
```

→ Crear o usuario de forma remota indicando o servidor LDAP

```
# samba-tool user setpassword anxo --newpassword=123passanxoABC
```

Modificar o contrasinal do usuario anxo do dominio, pois a opción random-password ten sentido para servizos (sen login)

```
# samba-tool group addmembers g-usuarios anxo,brais
```

→ Engadir ao grupo SAMBA g-usuarios os usuarios anxo e brais

```
# samba-tool group listmembers g-usuarios
```

→ Listar os membros pertencentes ao grupo SAMBA g-usuarios

```
# samba-tool user list
```

```
Administrator → Administrador do dominio
brais          → Conta de usuario pertencente ao grupo do dominio g-usuarios
Guest          → Invitado
krbtgt         → Usuario kerberos
anxo           → Conta de usuario pertencente ao grupo do dominio g-usuarios
```

Listar todos os usuarios SAMBA do controlador de dominio rexistrados no LDB(LDAP). Agora non se amosan os usuarios Samba: ana, xurxo, usuario, que xeramos con smbpasswd cando o servidor SAMBA posuía o rol Servidor Independente (Server Standalone) porque ao instalar Samba como Controlador de Dominio eliminouse toda a base de datos de usuarios antiga.

```
# samba-tool computer list
```

```
LSERVER1$
```

Listar todos os computadores.

→ *Os computadores, igual que os usuarios/grupos, tamén posúen conta no Directorio Activo do Dominio*

```
# samba-tool group removemembers g-usuarios anxo,brais
```

→ Eliminar do grupo SAMBA g-usuarios os usuarios anxo e brais

```
# samba-tool group delete g-usuarios
```

→ Eliminar o grupos SAMBA g-usuarios

```
# for i in anxo brais; do samba-tool user delete ${i};done
```

→ Eliminar os usuarios SAMBA anxo e brais

Listar usuarios/grupos

(pdbedit → evolución de smbpasswd)

(getent → /etc/nsswitch.conf → nscd)

(man 8 nscd)

(**nsld** → getent → ldap)



(/etc/nslcd.conf)

(man 5 nslcd.conf)

(man 8 nslcd)

(wbinfo → winbindd)

(man 8 winbindd)

(man 1 wbinfo)

```
# pdbedit -L
nobody:65534:nobody
LSERVER1$:4294967295:
brais:4294967295:
anxo:4294967295:
Administrator:4294967295:
krbtgt:4294967295:
# wbinfo -u && wbinfo -g
```

→

samba-tool user list

samba-tool computer list

Comandos similares aos anteriores para listar usuarios/grupos existentes en LDB(LDAP) Samba.

getent passwd && getent group

→

Listar usuarios/grupos existentes no sistema, os cales de momento NON inclúen os de LDB Samba. Polo tanto, anxo e brais, aínda que posúen conta LDB(LDAP) non poden acceder ao sistema xa que éste NON é quen de ler a base de datos LDB Samba.

```
# A=$(grep -n 'idmap' /etc/samba/smb.conf | cut -d':' -f1)
# sed -i "${A}a\\tldap server require strong auth = no\\n\\tacl:search = no"
/etc/samba/smb.conf
# systemctl restart samba-ad-dc
```

Configurar e Reiniciar servizo Samba para permitir autenticación sen cifrar

→ Instalar nslcd

```
# echo 'nslcd nslcd/ldap-uris string ldap://127.0.0.1/' | debconf-set-selections
# echo 'nslcd nslcd/ldap-base string dc=ies.local' | debconf-set-selections
# echo 'libnss-ldapd libnss-ldapd/nsswitch multiselect passwd, group, shadow' |
debconf-set-selections
# echo 'libnss-ldapd:amd64 libnss-ldapd/nsswitch multiselect passwd, group,
shadow' | debconf-set-selections
# apt -y install nslcd
```

```
# sed -i 's/base dc=ies.local/base dc=ies,dc=local/' /etc/nslcd.conf
# echo 'pagesize 1000
referrals off
binddn cn=Administrator,cn=Users,dc=ies,dc=local
bindpw abc123.
filter passwd (objectClass=user)
filter group (objectClass=group)
map passwd uid sAMAccountName
map passwd homeDirectory unixHomeDirectory
map passwd gecos displayName
map passwd gidNumber primaryGroupID
' >> /etc/nslcd.conf
# systemctl restart nslcd && systemctl restart nscd || reboot
```

nslcd: Integrar usuarios/grupos de LDB(LDAP) Samba no sistema Unix.

getent passwd && getent group

→

Listar usuarios/grupos existentes no sistema, os cales agora SI inclúen os de LDB Samba. Polo tanto, anxo e brais, que posúen conta LDB(LDAP) si poden acceder ao sistema xa que éste SI é quen de ler a base de datos LDB Samba.

Comprobar co usuario anxo que se accede mediante ttyX(tty1 -> anxo) e SSH(ssh anxo@lserver1)

Cientes de dominio

Cientes GNU/Linux
(Apuntar a DNS SAMBA)
(Cambiar hostname)

(Instalar/Configurar pbis)



(man 7 pbis)
(Unir/Quitar domainjoin-cli)



lserver1 → Identifica o hostname(fqdn) ou a IP do Servidor Samba. \$HOME(/home/IES/username) (\$ /opt/pbis/bin/config --list)
lclient1 → Identifica o hostname do equipo cliente /opt/pbis/bin/config HomeDirTemplate %H/%D/%U
lcliente1.ies.local → Identifica o hostname FQDN do equipo cliente (reino kerberos) %H → /home %D → IES %U → username

Executar o seguinte script en cada host a ser cliente do dominio (Modificar lclient1 polo hostname que corresponda).

```
#Configurar como servidor DNS o servidor Samba4
f_DNS() {
    echo -e "domain ies.local\nsearch ies.local\nnameserver 172.16.10.254" > /etc/resolv.conf
}

#Modificar hostname a FQDN apuntando ao servidor DNS Samba4
f_modify_hostname(){
    echo 'lclient1.ies.local' > /etc/hostname && sed -i 's/lclient1/lclient1.ies.local lclient1/' /etc/hosts
    grep 'lclient1.ies.local' /etc/sysctl.conf
    [ $? -ne 0 ] && echo 'kernel.hostname=lclient1.ies.local' >> /etc/sysctl.conf
    sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
    [ $(hostname -f) != 'lclient1.ies.local' ] && exit 55
    if [ $? -eq 55 ]; then
        echo '##### 0 hostname é incorrecto #####'
    fi
}

#Instalar pbis para poder unir/quitar clientes do dominio
f_install_pbis() {
    apt -y install gpgv2 wget
    wget -O - http://repo.pbis.beyondtrust.com/apt/RPM-GPG-KEY-pbis | apt-key add - \
    && wget -O /etc/apt/sources.list.d/pbiso.list http://repo.pbis.beyondtrust.com/apt/pbiso.list
    apt update && apt -y install pbis-open
}

#Configurar contas: Permitir facer login sen empregar nome dominio, umask 077, /bin/bash ($ /opt/pbis/bin/config --list)
f_config_pbis(){
    /opt/pbis/bin/config AssumeDefaultDomain true
    /opt/pbis/bin/config UserDomainPrefix IES
    /opt/pbis/bin/config HomeDirUmask 077
    /opt/pbis/bin/config LoginShellTemplate /bin/bash
}

f_main() {
    f_DNS && f_modify_hostname && f_install_pbis && f_config_pbis
}

##main()
f_main
```

apt -y install openssh-server

→ Instalar o paquete openssh-server

domainjoin-cli join IES.LOCAL Administrator abc123. && reboot

Unir o equipo onde se executa o comando ao dominio.
Unha vez reiniciado comprobar co usuario anxo que se accede mediante ttyX(tty1 -> anxo), su(su - anxo) e SSH(ssh anxo@lserver1)

domainjoin-cli leave Administrator@IES.LOCAL abc123.

→ Quitar o equipo onde se executa o comando ao dominio

No Servidor

samba-tool computer list

→ Listar equipos do dominio

samba-tool computer show LCLIENT1\$

→ Amosar o obxeto computadora LCLIENT1\$ do dominio

samba-tool computer delete LCLIENT1\$

→ Eliminar conta equipo LCLIENT1\$ do dominio

No Cliente de dominio(lclient1) → Verificar acceso de usuarios

- **Domain users (domain^users)** Todo usuario do dominio pertence a este grupo para poder acceder aos recursos compartidos.

anxo

Acceder mediante ttyX(tty7 -> anx) e SSH(ssh anx@lserver1). Comprobar que como anteriormente cambiamos o contrasinal non se solicita o cambio no inicio de sesión. Unha vez iniciada sesión executar:

```
$ id anx → Imprime UIDs e GIDs reais e efectivos
$ groups anx → Imprime os grupos nos que está o usuario anx
```

```
anxo@lclient1:~$ id anx
uid=1843922004(anxo) gid=1843921409(domain^users) grupos=1843921409(domain^users),1843922003(g-usuarios)
anxo@lclient1:~$ groups anx
anxo : domain^users g-usuarios
```

brais

Acceder mediante ttyX(tty7 -> brais) e SSH(ssh brais@lserver1). Verificar que agora ao usuario brais solicítaselle o cambio de contrasinal no primeiro inicio de sesión como se definiu na creación da conta. Unha vez iniciada sesión executar:

```
$ id brais → Imprime UIDs e GIDs reais e efectivos
$ groups brais → Imprime os grupos nos que está o usuario brais
```

```
brais@lclient1:~$ id brais
uid=1843922005(brais) gid=1843921409(domain^users) grupos=1843921409(domain^users),1843922003(g-usuarios)
brais@lclient1:~$ groups brais
brais : domain^users g-usuarios
```

No Servidor → Xestionar arrays de discos: RAID5(/dev/md5), RAID0(/dev/md0)

No Servidor

(mdadm)

(man mdadm.conf)

(man update-initramfs)

sda: Disco duro do sistema

sd[bcde]: Discos para montaxe de arrays

sdb1

sdb2

sdc1

sdc2

sdd1

sdd2

sde1

sde2

RAID5(/dev/md5): 4 discos/particións

3 sincronizados(sd[bcd]1) + 1 en espera(sde1)
/dev/md5 → /mnt/md5

RAID0(/dev/md0): 4 discos/particións (sd[bcde]2)

/dev/md0 → /mnt/md0

```
$ mount || findmnt
$ cat /proc/mdstat
# mdadm --detail /dev/md5
# mdadm --detail /dev/md0
# ls -lR /mnt/md5 /mnt/md0
# mkdir /mnt/md0/temporal
# mkdir -p /mnt/md5/usuarios/alumnos
# mkdir -p /mnt/md5/usuarios/profesores
# #Comando chgrp
#Necesario facer o apartado Prerrequisitos ACLS Servidor
##chgrp -R "Domain Admins" /mnt/md0/temporal /mnt/md5/usuarios
# chmod 0775 /mnt/md0/temporal
# chmod 2750 /mnt/md5/usuarios
# apt -y install tree
# tree -a /mnt/md5 /mnt/md0
/mnt/md5
├── lost+found
├── usuarios
│   ├── alumnos
│   └── profesores
/mnt/md0
├── lost+found
└── temporal
# ls -lR /mnt/md5 /mnt/md0
```

Comprobar que os arrays RAID5(/dev/md5) e RAID0(/dev/md0) son funcionais e xerar cartafoles dentro dos arrays para empregalos como Recursos Compartidos:
[usuarios]
[temporal]

Recursos Compartidos nos arrays de discos: RAID5(usuarios), RAID0(temporal)

- **Domain users (domain^users)** Todo usuario do dominio pertence a este grupo para poder acceder aos recursos compartidos.

- **SeDiskOperatorPrivilege** Só os usuarios e grupos que teñan o privilexio SeDiskOperatorPrivilege concedido poden configurar os permisos para compartir. Suxírese crear un novo grupo AD "Unix Admins" e engadir o seu gidNumber ao grupo Administrators, para logo empregar ese grupo en Unix onde usaría normalmente Domain Admins.

[usuarios]

comment = Cartafol dos usuarios → Descrición da sección a visualizar
Accédese ao recurso compartido /mnt/md5/usuarios/ mediante o nome da sección usuarios
mkdir /mnt/md5/usuarios && chgrp -R "Domain Admins" /mnt/md5/usuarios && chmod 2750 /mnt/md5/usuarios

path = /mnt/md5/usuarios → #Necesario facer o apartado **Prerrequisitos ACLS Servidor**
Non empregar homes como nome da sección a compartir (ver Introduction)
De interese: Roaming Windows User Profiles

read only = no → Permisos de escritura
guest ok = no → Acceso permitido soamente aos usuarios autenticados

force create mode = 0600 → Controla permisos ugo no lado do servidor. Obriga a Samba a crear os novos ficheiros dentro do recurso compartido(path) mediante os permisos ugo 600 (u g o = rw- --- ---).

force directory mode = 0700 → Controla permisos ugo no lado do servidor. Obriga a Samba a crear os novos directorios dentro do recurso compartido(path) mediante os permisos 700 (u g o = rwx --- ---).

[temporal]

comment = temporal. → Descrición da sección a visualizar. Este recurso: Bórrase todos os días (Tarefa Programada: /etc/crontab). Alumnos: Permisos de Lectura. Profesores: Permisos de escritura.
Ruta do recurso compartido

path = /mnt/md0/temporal → # mkdir /mnt/md0/temporal && chgrp -R 'Domain Admins' /mnt/md0/temporal && chmod 2750 /mnt/md0/temporal #Necesario facer o apartado **Prerrequisitos ACLS Servidor**

browseable = yes → Este recurso compartido é accesible ao explorar a rede.

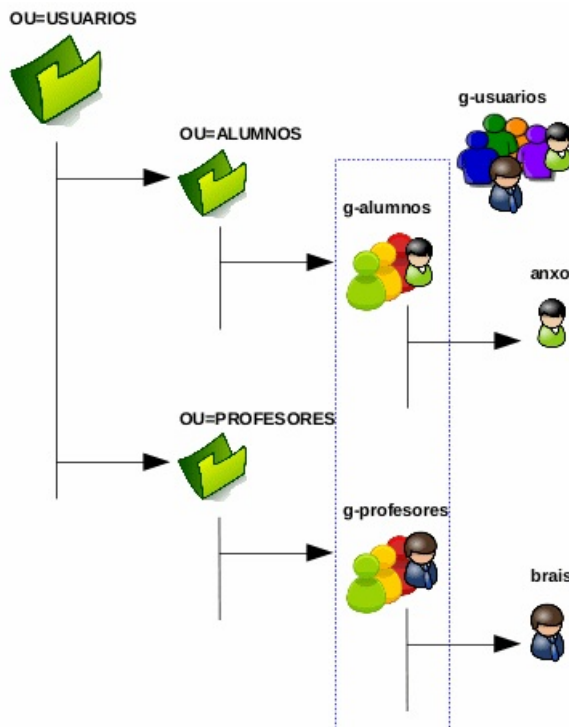
read only = no → Permisos de escritura

create mask = 0660 → Máximo nivel de permisos dos ficheiros a crear dentro do cartafol /mnt/md0/temporal (u g o = rw- rw- ---). Controla permisos ugo no lado do servidor.

directory mask = 0770 → Máximo nivel de permisos dos directorios a crear dentro do cartafol /mnt/md0/temporal (u g o = rwx rwx ---). Controla permisos ugo no lado do servidor.

No Servidor

testparm → Verificar ficheiro de configuración Samba
smbcontrol all reload-config → Recargar configuración Samba



LDAP (ldb-tools) (ldif)

O paquete `ldb-tools` ofrece unha serie de comandos para a administración de datos no directorio LDAP. Os comandos para engadir, modificar, buscar, eliminar, editar e renomear son respectivamente: `ldbadd`, `ldbmodify`, `ldbsearch`, `ldbdel`, `ldbedit` e `ldbrename`. Permiten ser empregados con arquivos LDIF e posúen unha sintaxe similar aos comandos `openldap`, do paquete `ldap-utils`, equivalentes (`ldapadd`, `ldapmodify`, `ldapsearch`, `ldapdelete` ...).

OU → Unidade Organizativa

`ldbmodify -H ldap://localhost -`

`Uadministrator%abc123. create-OU-2.ldif`

→ Crear OU a través do
arquivo `create-OU-2.ldif`

Arquivos LDIF

create-OU-2.ldif

`dn: OU=alumnos,OU=usuarios,OU=ies,DC=ies,dc=local`

`changetype: add`

`objectClass: top`

`objectClass: organizationalunit`

`description: alumnos OU`

`dn: OU=profesores,OU=usuarios,OU=ies,DC=ies,dc=local`

`changetype: add`

`objectClass: top`

`objectClass: organizationalunit`

`description: profesores OU`

Usuarios/Grupos

samba-tool → evolución de `pdbedit` → evolución de `smbpasswd`

~~# samba-tool group add g-usuarios \~~
~~--groupou=OU=USUARIOS,OU=IES --nis-domain=ies --gid-number=10000~~

→ Crear grupo `g-usuarios` no dominio SAMBA. Pero xa deberíamos telo creado.

`samba-tool group add g-alumnos \`
`--groupou=OU=ALUMNOS,OU=USUARIOS,OU=IES --nis-domain=ies \`
`--gid-number=10001`

→ Crear grupo `g-alumnos` no dominio SAMBA

`samba-tool group add g-profesores \`
`--groupou=OU=PROFESORES,OU=USUARIOS,OU=IES --nis-domain=ies \`
`--gid-number=10002`

→ Crear grupo `g-profesores` no dominio SAMBA `g-profesores`

`samba-tool group addmembers g-usuarios g-alumnos,g-profesores` → Engadir ao grupo do dominio SAMBA `g-usuarios` os grupos `g-alumnos` e `g-profesores`

`samba-tool group addmembers g-alumnos anxo` → Engadir ao grupo do dominio SAMBA `g-alumnos` o usuario `anxo`

`samba-tool group addmembers g-profesores brais` → Engadir ao grupo do dominio SAMBA `g-alumnos` o usuario `brais`

`samba-tool group listmembers g-usuarios` → Listar membros pertencentes ao grupo do dominio SAMBA `g-usuarios`

`samba-tool group listmembers g-alumnos` → Listar membros pertencentes ao grupo do dominio SAMBA `g-alumnos`

`samba-tool group listmembers g-profesores` → Listar membros pertencentes ao grupo do dominio SAMBA `g-profesores`

Prerrequisitos ACLs

1. **Soporte para ACLs estendido nos sistemas de ficheiros:** Hoxe en día o kernel trae incorporado por defecto soporte para ACLs para distintos sistemas de ficheiros. Podemos verificalo co seguinte comando:

```
# [ -f /boot/config-$(uname -r) ] && grep -i acl /boot/config-$(uname -r)
CONFIG_EXT4_FS_POSIX_ACL=y
CONFIG_REISERFS_FS_POSIX_ACL=y
...
```

Pero no caso que así non sexa debemos activar no sistema de ficheiros o soporte para as ACLs, polo que deberiamos instalar o paquete **acl** e modificar o arquivo **/etc/fstab**:

```
# apt update && apt -y install acl
# cat /etc/fstab | nl
...
7 # <file system> <mount point> <type> <options> <dump> <pass>
8 # / was on /dev/sda1 during installation
9 UUID=3e1ae11e-dac7-4a58-8aec-d06a345171dc / ext4 acl,errors=remount-ro 0 1
...
```

No cuarto campo do ficheiro **/etc/fstab** correspondente aos opcións de montaxe debemos agregar a opción **acl** e posteriormente debemos remontar o sistema de ficheiros modificado. Para non ter que reiniciar podemos empregar calquera dos 2 seguintes comandos:

```
# mount -a #Remonta todos os sistemas de ficheiros seguindo a orde en /etc/fstab
# mount -o remount /dev/sda1 #Remonta soamente o sistema de ficheiros modificado en /etc/fstab (neste caso /dev/sda1)
```

2. **Soporte para ACLs estendido de Samba,** é dicir, Samba foi instalado co soporte ACL estendido habilitado.

```
# smb -b | grep "HAVE_LIBACL"
HAVE_LIBACL
```

Se non amosa saída → **Dependencias paquete Samba**



Un host Samba que funciona como AD-DC sempre está habilitado con soporte ACL estendido:

testparm → [global] → vfs objects → acl_xattr

3. É necesario establecer o **gidNumber** de "Domain Admins" para poder traballar as ACLs con este grupo.

```
# ldbmodify -H ldap://localhost -Uadministrator%abc123. modify-gidNumber.ldif
```

modify-gidNumber.ldif

```
dn: CN=Domain Admins,CN=Users,DC=ies,DC=local
changetype: modify
replace: gidNumber
gidNumber: 12000
```

Ao configurar o recurso compartido nun controlador de dominio (DC) de Samba Active Directory (AD), non pode usar ACL POSIX. Nun Samba DC, só se admiten comparticións que usan ACL estendidas. Consulte:

- **Activar a asistencia ACL estendida no ficheiro smb.conf.**
- **Configuración do uso compartido de cartafol domésticos no servidor de ficheiros Samba - Usando ACL de Windows.**

ACLs para o recurso compartido [usuarios]

```
mkdir -p /mnt/md5/usuarios/alumnos /mnt/md5/usuarios/profesores
chgrp -R "Domain Admins" /mnt/md5/usuarios/
chmod 2770 /mnt/md5/usuarios/
```

```
setfacl -m g:g-usuarios:rwX /mnt/md5/usuarios
setfacl -m g:"Domain Admins":rwX /mnt/md5/usuarios
setfacl -dm g:"Domain Admins":rwX /mnt/md5/usuarios
```

```
setfacl -m g:"Domain Admins":rwX /mnt/md5/usuarios/alumnos
setfacl -m g:g-profesores:rx /mnt/md5/usuarios/alumnos
setfacl -m g:g-alumnos:rx /mnt/md5/usuarios/alumnos
```

```
setfacl -m g:"Domain Admins":rwX /mnt/md5/usuarios/profesores
setfacl -m g:g-profesores:rx /mnt/md5/usuarios/profesores
setfacl -m g:g-alumnos:--- /mnt/md5/usuarios/profesores
setfacl -dm o:--- /mnt/md5/usuarios/profesores
setfacl -dm g:--- /mnt/md5/usuarios/profesores
```

Usuarios pertencentes ao grupo g-alumnos: Crear cartafol + ACLs

```
mkdir -p /mnt/md5/usuarios/alumnos/anxo
setfacl -m u:anxo:rwX /mnt/md5/usuarios/alumnos/anxo
setfacl -dm u:anxo:rwX /mnt/md5/usuarios/alumnos/anxo
```

Usuarios pertencentes ao grupo g-profesores: Crear cartafol + ACLs

```
mkdir -p /mnt/md5/usuarios/profesores/brais
setfacl -m u:brais:rwX /mnt/md5/usuarios/profesores/brais
setfacl -dm u:brais:rwX /mnt/md5/usuarios/profesores/brais
```

ACLs para o recurso compartido [temporal]

```
# mkdir -p /mnt/md0/temporal
# chgrp -R "Domain Admins" /mnt/md0/temporal/
# chmod 2750 /mnt/md0/temporal/
# setfacl -m g:g-profesores:rwX /mnt/md0/temporal/
# setfacl -dm g:g-profesores:rwX /mnt/md0/temporal/
# setfacl -m g:g-alumnos:rx /mnt/md0/temporal/
# setfacl -dm g:g-alumnos:rx /mnt/md0/temporal/
```

- Crear cartafol /mnt/md0/temporal
- Asignar, recursivamente, a "Domain Admins" como grupo propietario
- Cambiar permisos ugo (rwX r-s ---). O permiso 2000(SGID) provoca que cada subdirectorio xerado continúe tendo como grupo propietario "Domain Admins"
- ACL estendida: Permisos rwX ao grupo g-profesores no cartafol /mnt/md0/temporal
- ACL estendida: Herdanza de Permisos rwX ao grupo g-profesores para calquera ficheiro/cartafol a crear dentro de /mnt/md0/temporal
- ACL estendida: Permisos rx ao grupo g-alumnos no cartafol /mnt/md0/temporal
- ACL estendida: Herdanza de Permisos rx ao grupo g-alumnos para calquera ficheiro/cartafol a crear dentro de /mnt/md0/temporal

Revisar ACLs

```
# getfacl -R /mnt/md5/usuarios/ && /mnt/md0/temporal/
```

Tarefa programada: Eliminar diariamente contido do recurso [temporal]

No servidor
(/etc/crontab)
(man 1 crontab)
(man 5 crontab)

```
# echo '@daily root rm -rf /mnt/md0/temporal/*' >> /etc/crontab → Eliminar todos os días as 00:00h o contido do cartafol /mnt/md0/temporal
```

(Des)Montar Recursos Compartidos → libpam_mount → login/logout

pam_mount → Os usuarios do dominio (AD Samba) non teñen que existir no cliente como usuarios Unix.

Imos montar no login e desmontar no logout.

- **libpam-mount** (man pam_mount && man pam_mount.conf)(/etc/security/pam_mount.conf.xml)(~/pam_mount.conf.xml)
- **%(USER):** Variable pam_mount. Identifica user_samba/uid_user_samba respectivamente. **Non se modifican**

```
# smbpasswd -a user_samba || samba-tool user setpassword user_samba --newpassword=123passuser_sambaABC  
# /opt/pbis/bin/config HomeDirTemplate %H/%D%U → actualizar $HOME a /home/IES/user_samba
```

```
<volume sgrp="g-alumnos" fstype="cifs" server="lserver1"  
path="usuarios/alumnos/%(USER)" mountpoint="/home/local/IES/%  
(USER)/Documentos"  
options="nodev,nosuid,workgroup=IES,file_mode=0640,dir_mode=0750"  
>
```

anxo pertence a g-alumnos → pode montar o recurso → permisos de montaxe no lado do cliente → file_mode=640, dir_mode=750 → permisos de escritura → ACLs no lado do servidor → soamente anxo permiso de escritura

Engadir en /etc/security/pam_mount.conf.xml para montar no login o recurso compartido [usuarios](path). sgrp → Limita o volume aos usuarios que son membros do grupo g-alumnos (independentemente sexa grupo primario ou secundario). **Este grupo g-alumnos é un grupo existente no dominio Samba.**

```
<volume sgrp="g-profesores" fstype="cifs" server="lserver1"  
path="usuarios/profesores/%(USER)" mountpoint="/home/local/IES/%  
(USER)/Documentos" options="nodev,nosuid,workgroup=IES,uid=%  
(USER)" >
```

brais pertence a g-profesores → pode montar o recurso → permisos de montaxe no lado do cliente → uid=%(USER) → permisos de escritura → ACLs no lado do servidor → soamente brais permiso de escritura

Engadir en /etc/security/pam_mount.conf.xml para montar no login o recurso compartido [usuarios](path). sgrp → Limita o volume aos usuarios que son membros do grupo g-profesores (independentemente sexa grupo primario ou secundario). **Este grupo g-profesores é un grupo existente no dominio Samba.**

```
<volume sgrp="g-usuarios" fstype="cifs" server="lserver1"  
path="temporal" mountpoint="/mnt/%(USER)/temporal"  
options="nodev,nosuid,workgroup=IES,file_mode=0600,dir_mode=0700"  
>
```

anxo, brais pertencen a g-usuarios → poden montar o recurso → permisos de montaxe no lado do cliente → file_mode=600, dir_mode=700 → permisos de escritura → ACLs no lado do servidor → soamente g-profesores permiso de escritura → soamente brais posúe permisos de escritura

Engadir en /etc/security/pam_mount.conf.xml para montar no login o recurso compartido [temporal](path=/mnt/md0/temporal en /mnt/\${USER}/temporal). sgrp → Limita o volume aos usuarios que son membros do grupo g-usuarios (independentemente sexa grupo primario ou secundario). **Este grupo g-usuarios é un grupo existente no dominio Samba.**

Iniciar sesión cos usuarios anxo, brais e probar a creación de ficheiros/directorios (gvfs-backends → thunar). *Comprobar no cliente e no servidor.*

No
Cliente

Cotas de usuario (soft/hard)

quota
(/etc/fstab →
usrquota,grpquota)

# apt -y install quota	→ Instalar o paquete quota
for i in \$(grep -nE 'md5 md0' /etc/fstab cut -d':' -f1 xargs);do sed -i "\${i} s/defaults/defaults,usrquota,grpquota/g" /etc/fstab;done	→ Incorporar cotas aos puntos de montaxe /dev/md5 e /dev/md0
# mount -o remount /mnt/md5 # mount -o remount /mnt/md0	→ Remontar os arrays para ter en conta as cotas
# quotacheck -avug	Chequear e ver (-v) a máxima información de todos (-a) os sistemas de ficheiros con cotas de usuarios (-u) e grupos (-g). No caso que non existen os ficheiros necesarios para activar as cotas: aquota.user e aquota.group no raíz de cada sistema de ficheiros comprobados, entón créaos.
# quotaon -av	→ Activar as cotas
# setquota -h	→ Ver a axuda do comando setquota
# setquota -u anxo 180000 200000 0 0 /mnt/md5	Establecer as cotas de bloques (espazo en disco) e as cotas de inodos (número de ficheiros). Así, establece para o usuario anxo as seguintes cotas de bloques: cota branda(soft) de 180000KB, cota dura(hard) de 200000KB e sen cotas de inodos para o sistema de ficheiros /dev/md5
# edquota -h	→ Ver a axuda do comando edquota
# edquota -u anxo	→ Editar as cotas do usuario anxo
# edquota -uT anxo	→ Editar o período de graza para o usuario anxo
# edquota -t	→ Editar o período de graza para todos
# setquota -u anxo 0 0 0 0 /mnt/md5	→ Eliminar as cotas do usuario anxo en /mnt/md5
# quota anxo	→ Verificar as quotas do usuario anxo
# repquota -a	→ Verificar as quotas en todos os sistemas de ficheiros
# repquota -av	→ Verificar as quotas en todos os sistemas de ficheiros. Tamén amosa usuarios e grupos sen o uso das súas quotas activadas.

Scripts de ejecución no inicio de sesión

Configuración no Host cliente

(/etc/netlogon/user/script
→ /etc/profile)

```
# mkdir -p /etc/netlogon/user
```

→ Crear o cartafol /etc/netlogon/user

```
# cat > /etc/netlogon/user/script_01.sh <<EOF
```

```
#!/bin/bash
```

```
if (groups ${u} | grep g-usuarios);then
```

```
data=$(date +%F-%H_%M)
```

→ Xerar script a executar

```
touch /tmp/file-${data}
```

```
fi
```

```
EOF
```

```
# echo 'bin/bash /etc/netlogon/user/script_01.sh' >> /etc/profile
```

Engadir en /etc/profile a execución do script.
→ No próximo inicio de sesión executarase o script

```
# su - anxo
```

```
domain^users g-usuarios
```

```
anxo@lclient1:~$ ls -l /tmp/
```

```
total 0
```

→ Comprobar iniciando sesión co usuario anxo

```
-rw-r--r-- 1 anxo domain^users 0 Xan 4 19:53 file-2020-01-04-19_53
```