

Cheat-Sheet: Samba4 Debian GNU/Linux

Samba4: Integra DNS, LDAP e Kerberos Heimdal

AD DC (Active Directory Domain Controller)

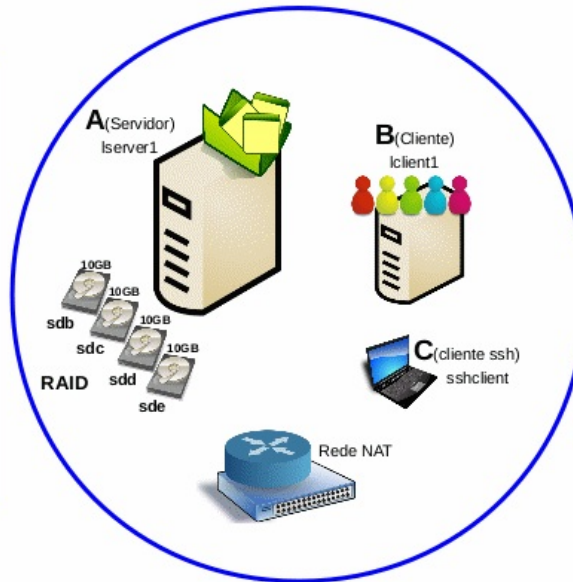
Update: 20240508

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

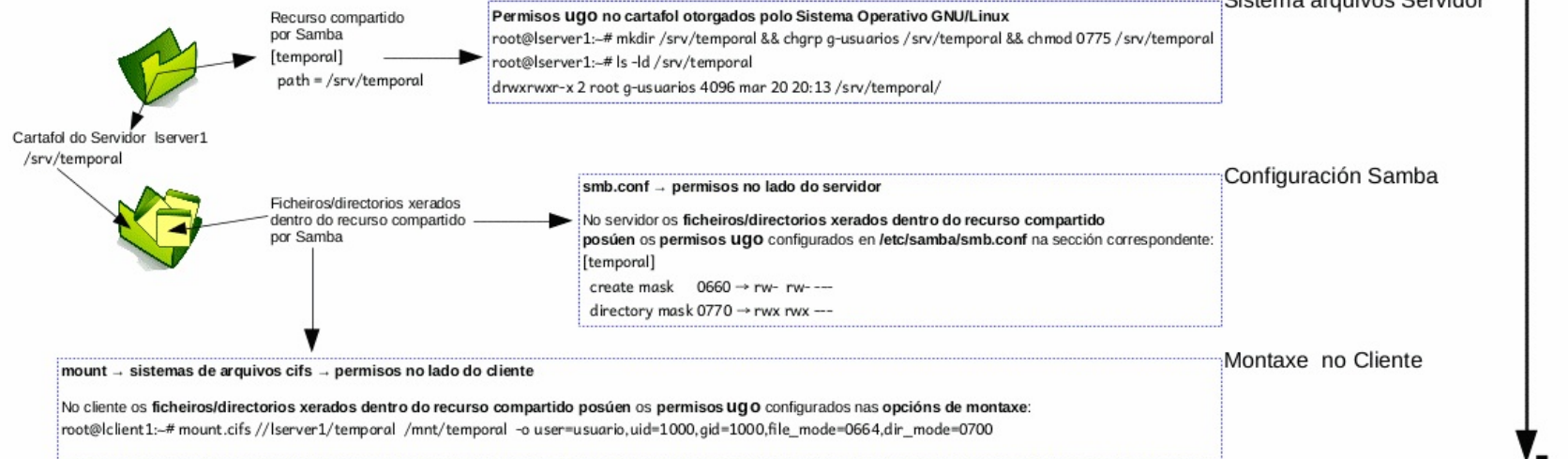
A: 172.16.10.254/24 Debian 64bits NTP, SAMBA4 (DNS,LDAP,KERBEROS) Hostname: lserver1 Servidor SSH sda: SO instalado sd[bcd]: array de discos	B: 172.16.10.150/24 Debian 64bits Hostname: lclient1 Servidor SSH
	C: 172.16.10.2/24 Debian 64bits + XFCE Cliente SSH Hostname: sshclient

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



Ricardo Feijoo Costa



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

Servidor Independente



Instalación

```
# echo 'samba-common samba-common/dhcp boolean false' | debconf-set-selections
# dpkg -l samba ; [ $? -ne 0 ] && apt update && apt -y install samba
```

Configurar na preinstalación do paquete
→ samba: Non empregar a configuración WINS de DHCP
→ Instalar SAMBA

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.
[homes] → Sección **opcional** correspondente á configuración dos cartafolios /home ou persoais dos usuarios
[printers] → Sección **opcional** correspondente á configuración de impresoras
[print\$] → Sección **opcional** destinada a compartir os drivers de impresoras existentes na seccións [printers]

```
# apt -y install moreutils
# grep -vE '^#|^;'
/etc/samba/smb.conf | sed -e '/^$/d' |
 sponge /etc/samba/smb.conf
```

[global]

```
workgroup = WORKGROUP
log file = /var/log/samba/log.%m
max log size = 1000
logging = file
panic action = /usr/share/samba/panic-action %d
```

→ Nome do grupo de traballo do equipo
→ Empregar un arquivo log por máquina que conecta (%m)
→ Limitar tamaño arquivo log a 1000kiB
→ Enviar rexistros de Samba a /var/log/samba/log.{smbd,nmbd}
→ Acción cando Samba ten problema: Enviar correo co problema ao admin de Samba
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 **servidor independente**.
Para executar como "active directory domain controller" requírese executar:
samba-tool domain provision || samba-tool domain provision --use-rfc2307 --interactive

```
server role = standalone server
```

→ Indica que Samba debe obedecer aos tipos account e session de PAM.
→ Sincronizar Unix password e SMB password cando SMB password cambia.

```
obey pam restrictions = yes
```

```
unix password sync = yes
```

```
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n
*Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .
```

→ Opcións necesarias para que a sincronización de Unix password funcione nun sistema Debian GNU/Linux

```
pam password change = yes
```

→ PAM para cambios de password dun cliente SMB

```
map to guest = bad user
```

→ Autenticacións fallidas son mapeadas a conexións anónimas

```
usershare allow guests = yes
```

→ Usuarios non autenticados poden acceder a recursos compartidos por un usuario

[homes]

comment = Home Directories → Descripción da sección a visualizar
browseable = no → Este recurso compartido non se amosa ao explorar a rede.
read only = yes → Permisos de só lectura
create mask = 0700 → Máximo nivel de permisos dos ficheiros a crear dentro do cartafol do usuario (u g o = rwx --- ---).
→ Controla permisos ugo no lado do servidor.
directory mask = 0700 → Máximo nivel de permisos dos directorios a crear dentro do cartafol do usuario (u g o = rwx --- ---).
→ Controla permisos ugo no lado do servidor.
valid users = %S → %S → os usuarios acceden ao seu cartafol persoal:
user_samba → /home/user_samba → \\server\user_samba

[printers]

comment = All Printers → Descripción da sección a visualizar
browseable = no → Este recurso compartido non se amosa ao explorar a rede.
path = /var/tmp → Accédese ao recurso compartido /var/tmp mediante o nome da sección printers.
printable = yes → Recurso compartido impresora está dispoñible
guest ok = no → Acceso permitido soamente aos usuarios autenticados
read only = yes → Permisos de só lectura
create mask = 0700 → Máximo nivel de permisos dos ficheiros a crear dentro do cartafol definido na directiva path
(u g o = rwx --- ---). Controla permisos ugo no lado do servidor.

[print\$]

comment = Printer Drivers → Descripción da sección a visualizar
path = /var/lib/samba/printers → Ruta do recurso compartido onde se comparten os drivers de impresoras a descargar para clientes
Windows.
browseable = yes → Este recurso compartido é accesible ao explorar a rede.
read only = yes → Permisos de só lectura
guest ok = no → Acceso permitido soamente aos usuarios autenticados

Crear recurso compartido temporal (escritura)

[temporal]

comment = temporal

path = /srv/temporal

browseable = yes

read only = no

create mask = 0660

directory mask = 0770

- Descripción da sección a visualizar
- Ruta do recurso compartido
 - # mkdir /srv/temporal && chgrp g-usuarios /srv/temporal && chmod 0775 /srv/temporal
- Este recurso compartido é accesible ao explorar a rede.
- Permisos de escritura
- Máximo nivel de permisos dos ficheiros a crear dentro do cartafol /srv/temporal (u g o = rw- rw- ---). Controla permisos ugo no lado do servidor.
- Máximo nivel de permisos dos directorios a crear dentro do cartafol /srv/temporal (u g o = rwx rwx ---). Controla permisos ugo no lado do servidor.

Crear recurso compartido descargas (só lectura)+(validación usuarios/grupos/hosts)

[descargas]

comment = descargas

path = /srv/descargas

browseable = yes

read only = yes

guest ok = no

valid users = ana, @g-usuarios

invalid users = xurxo, @g-external

hosts allow = 127.0.0.1 172.16.10.0/24 lclient1

hosts deny = 172.16.10.150 lclient2

- Descripción da sección a visualizar
- Ruta do recurso compartido
 - # mkdir /srv/descargas && chgrp g-usuarios /srv/descargas && chmod 2770 /srv/descargas
- Este recurso compartido é accesible ao explorar a rede.
- Permisos de só lectura
- Acceso permitido soamente aos usuarios autenticados
- Acceso permitido ao usuario ana e ao grupo g-usuarios.
- Acceso non permitido ao usuario xurxo e ao grupo @g-external. **invalid users prevalece no caso de conflito con valid users**
- Acceso permitido á dirección IP 127.0.0.1, á rede 172.16.10.0/24 e ao host lclient1
- Acceso non permitido aos host 172.16.10.150 e lclient2
 - **hosts allow prevalece no caso de conflito con hosts deny**
 - **hosts deny prevalece no caso de conflito con valid users**

Servizo/s

(smbd
&&
nbmd)

(man 8 smbd

&&

man 8 nbmd)

(samba-ad-dc

&&

winbind)

(man 8 winbindd)

Servidor Independente: smbd && nbmd

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

systemctl status smbd && systemctl status nbmd → Ver estado

systemctl start smbd && systemctl start nbmd → Arrancar

systemctl stop smbd && systemctl stop nbmd → Parar

systemctl reload smbd && systemctl reload nbmd → Recargar

smbcontrol all reload-config → Recargar

smbd → Xestiona a funcionalidade principal de compartir ficheiros e impresoras, atendendo as solicitudes de clientes SMB/CIFS

nbmd → Xestiona a resolución de nomes NetBIOS a IP, permitindo que os clientes atopen os recursos compartidos na rede.

Controlador de dominio: samba-ad-dc

samba-ad-dc → Cando configuramos Samba como AD-DC debemos instalar winbind e arrancar samba-ad-dc

winbind → Xestiona a integración de sistemas Unix/Linux nun entorno de rede baseado en AD, permitindo autenticación de usuarios e resolución de nomes en AD.

apt -y install winbind → Instalar winbind

systemctl status samba-ad-dc → Ver estado

systemctl stop smbd && systemctl stop nbmd → Parar smbd && nbmd

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)

smbpasswd

(man 8 smbpasswd)

(man 5 smbpasswd)

(1) Debe existir: user → usuario Unix

useradd -m -d /home/user -p \$(mkpasswd -m sha-512 abc123.) -s /bin/bash user

Non se require shell válida nin cartafol de usuario, pero si un contrasinal de sistema que habilite a conta Unix. Se a conta de sistema Unix está deshabilitada Samba non permite o acceso. Así, poderíase crear o usuario:

apt -y install whois && useradd -M -s /usr/sbin/nologin -p \$(mkpasswd -m sha-512 abc123.) user

Pode engadirse ese usuario nun grupo:

groupadd g-usuarios

usermod -aG g-usuarios user

```
# useradd -M -s /usr/sbin/nologin -p $(mkpasswd -m sha-512 abc123.) ana
# useradd -M -s /usr/sbin/nologin -p $(mkpasswd -m sha-512 abc123.) xurxo
# groupadd g-usuarios
# usermod -aG g-usuarios ana
# groupadd g-external
# usermod -aG g-external xurxo
```

(2) Unha vez exista conta de usuario Unix pódese xerar user_samba → usuario Samba (o contrasinal Samba non ten porque ser o mesmo que o do sistema Unix)

smbpasswd -a user → Engadir usuario a SAMBA e establecer o seu contrasinal SAMBA

smbpasswd -a user_samba → Cambiar contrasinal SAMBA. Para deixar o mesmo contrasinal SAMBA premer ↵

smbpasswd -x user_samba → Eliminar usuario SAMBA

smbpasswd -d user_samba → Deshabilitar usuario SAMBA

smbpasswd -e user_samba → Habilitar usuario SAMBA

Listar usuarios/grupos

(pdbedit → evolución de smbpasswd)

(getent → /etc/nsswitch.conf)

(man getent)

(man nsswitch.conf)



pdbedit -Lv

→ Listar usuarios existentes en Samba

getent passwd && getent group

→ Listar usuarios/grupos existentes no sistema, sen incluír os pertencentes a un DOMINIO Samba

smbclient

lserver1 → Identifica o hostname(fqdn) ou a IP do Servidor Samba

apt -y install smbclient

→ Instalar

echo 172.16.10.254 lserver1 | tee -a /etc/hosts

smbclient -L //lserver1 -U%

→ Visualizar recurso/s compartido/s mediante acceso anónimo

smbclient -L //lserver1 -Uuser_samba

→ Visualizar recurso/s compartido/s mediante acceso autenticado

smbclient //lserver1/descargas -Uuser_samba → Acceder(console smb) a [descargas] mediante acceso autenticado

lserver1 → Identifica o hostname(fqdn) ou a IP do Servidor Samba

Sharelserver1 → Identifica o recurso compartido no Servidor Samba

FolderClient → Identifica o cartafol do Cliente Samba no que se terá acceso ao recurso compartido do Servidor Samba

/etc/fstab → Ficheiro automontaxe no arranque do sistema ou empregando o comando **mount -a**libpam-mount (/etc/security/pam_mount.conf.xml) → Configurar que o recurso compartido por CIFS poida **ser montado no login e desmontado no logout** sen ter que escribir as credenciais

WORKGROUP → Identifica o nome do grupo de traballo do equipo

cifs-utils (man mount.cifs && man mount)

apt -y install cifs-utils

→ Instalar

```
# mount -t cifs //lserver1/Sharelserver1 /mnt/FolderClient -o \
user=USER,uid=UID,gid=GID,file_mode=0660,dir_mode=0770
# mount.cifs //lserver1/Sharelserver1 /mnt/FolderClient -o \
user=USER,uid=UID,gid=GID,file_mode=0660,dir_mode=0770
```

Montar no cliente o recurso compartido. Comandos equivalentes.

apt -y install gvfs-backends

Alt+F2 --> thunar --> smb://lserver1/Sharelserver1

USER=user_samba, UID=uid_user_cliente,
 GID=gid_user_cliente, {file,dir}_mode → Controlan
 permisos ugo no lado do cliente. Debe existir
 /mnt/FolderClient (# mkdir -p /mnt/FolderClient)

Montar de xeito permanente no cliente o recurso compartido.

```
echo '//lserver1/Sharelserver1 /mnt/FolderClient cifs
user=USER,password=PASS,uid=UID,gid=GID,
file_mode=0660,dir_mode=0770 0 0' >> /etc/fstab
```

USER=user_samba, PASS=password_user_samba,
 UID=uid_user_cliente, GID=gid_user_cliente

[homes] → Para que funcionen os permisos rw:
mount → rw + [homes] → read only = no

```
# echo -e 'username=USER\npassword=PASS' >
/root/file_credentials.txt
```

chown root. /root/file_credentials.txt

chmod 400 /root/file_credentials.txt

```
# echo '//lserver1/Sharelserver1 /mnt/FolderClient cifs
credentials=/root/file_credentials.txt,uid=UID,gid=GID,
file_mode=0660,dir_mode=0770 0 0' >> /etc/fstab
```

Montar de xeito permanente no cliente o recurso
 compartido,
 empregando o ficheiro file_credentials.txt para
 → autenticación. Os permisos dese ficheiro son de só
 lectura para o usuario root.
 USER=user_samba, PASS=password_user_samba,
 UID=uid_user_cliente, GID=gid_user_cliente

libpam-mount (man pam_mount && man pam_mount.conf)(/etc/security/pam_mount.conf.xml)(~/pam_mount.conf.xml)%(USER), %(USERUID): Variables pam_mount. Identifican user_samba/uid_user_samba respectivamente. **Non se modifican**Para que funcione a compartición → **password user system = password user samba** → **smbpasswd -a user_samba**

apt -y install libpam-mount

→ Instalar

```
<volume pgrp="%(GROUP)" uid="%(USERUID)" fstype="cifs"
server="lserver1" path="homes" mountpoint="/mnt/%
(USER)" options="nodev,nosuid,workgroup=WORKGROUP,
iocharset=utf8,file_mode=0700,dir_mode=0700,vers=1.0" />
```

Montar no login o recurso compartido [homes](path)

→ (file_mode=0700 → Permisos ficheiros a crear rw- --- ---)

→ (dir_mode=0700 → Permisos directorios a crear rwx --- ---)

(Des)Montar

(u)mount
 (/etc/fstab)
 (pam_mount)

Exemplo: Verificación de Permisos UGO no lado do Servidor e no lado do Cliente

- Os permisos UGO no lado do Servidor veñen dados na configuración de Samba, é dicir, aínda que os permisos UGO poidan ser modificados na montaxe por un cliente Samba no servidor os ficheiros/directorios terán os permisos dados na configuración do recurso compartido de Samba.
- Os permisos UGO no lado do Cliente veñen dados polo cliente Samba a través do comando/app de montaxe (cifs.utils → mount → uid, gid, forceuid, forcegid, file_mode, dir_mode).
 - uid=number/username → identifica u de ugo pertencente ao cliente cando o servidor non proporciona esta información. Por defecto = 0
 - forceuid=number/username → obriga a identificar u de ugo pertencente ao cliente ignorando o uid proporcionado polo servidor.
 - gid=number/groupname → identifica g de ugo pertencente ao cliente cando o servidor non proporciona esta información. Por defecto = 0
 - forcegid=number/username → obriga a identificar g de ugo pertencente ao cliente ignorando o gid proporcionado polo servidor.
- Unha vez montado o recurso modificar no cliente os permisos cos comandos chmod, chown non darán erro pero non terán efecto.

[temporal]

comment = temporal

→ Descrición da sección a visualizar

path = /srv/temporal

→ Ruta do recurso compartido

mkdir /srv/temporal && chgrp g-usuarios /srv/temporal && chmod 0770 /srv/temporal

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 /srv/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 /srv/temporal (u g o = rwx rwx ---). Controla permisos ugo no lado do servidor.

No Cliente

ana → user_samba que non ten por que existir no cliente.

uid=1001, gid=1001 → uid/gid pertencentes ao cliente Samba. Se existen aparecerán os nomes e se non existen aparecerán números.

mkdir /mnt/temporal

mount.cifs //lserver1/temporal /mnt/temporal -o

user=ana,uid=1001,gid=1001,file_mode=0764,dir_mode=0755

No cliente os ficheiros xerados terán permisos ugo 764 e os directorios 755, aínda que no servidor os permisos destes ficheiros e directorios xerados serán 660 para ficheiros e 770 para directorios. Se soamente quixeramos que no cliente ana tivera permisos sobre os ficheiros e directorios xerados: file_mode=0600, dir_mode=0700

ls -ld /mnt/temporal

→ Revisar permisos do cartafol /mnt/temporal

mkdir /mnt/temporal/dir1-ana && touch /mnt/temporal/f1-ana.txt

→ Crear directorio e ficheiro

ls -l /mnt/temporal

→ Revisar permisos dentro do cartafol /mnt/temporal

No Servidor

ls -ld /srv/temporal → Revisar permisos do cartafol /srv/temporal

Revisar permisos dentro do cartafol /srv/temporal. Como cando creamos o recurso compartido /srv/temporal

ls -l /srv/temporal → executamos chmod 0775 /srv/temporal todos os ficheiros/directorios creados en /srv/temporal terán como user/group propietario o user/group propietario do usuario samba que monta o recurso e crea o ficheiro/directorio.

No Cliente

xurxo → user_samba que non ten por que existir no cliente. Grupos no servidor: pertence a g-external e non pertence a g-usuarios

umount /mnt/temporal

→ Desmontar recurso compartido

mount.cifs //lserver1/temporal /mnt/temporal -o

user=xurxo,uid=1001,gid=1001,file_mode=0764,dir_mode=0755 → Erro na montaxe pois xurxo non é ana, nin pertence ao grupo g-usuarios do servidor, polo tanto non ten acceso ao recurso compartido. (Verificar de novo tras executar no servidor: # usermod -aG g-usuarios xurxo)(Tras verificar eliminar a pertenza ao grupo: # gpsswd -d xurxo g-usuarios)

Exemplo: Verificación de control de Usuarios/Grupos/Hosts

[descargas]

comment = descargas

path = /srv/descargas

browseable = yes

read only = yes

guest ok = no

valid users = ana, @g-usuarios

invalid users = xurxo, @g-external

hosts allow = 127.0.0.1 172.16.10.0/24 lclient1

hosts deny = 172.16.10.150 lclient2

→ Descripción da sección a visualizar

Ruta do recurso compartido

→ # mkdir /srv/descargas && chgrp g-usuarios /srv/descargas && chmod 2770 /srv/descargas

→ Este recurso compartido é accesible ao explorar a rede.

→ Permisos de só lectura

→ Acceso permitido soamente aos usuarios autenticados

→ Acceso permitido ao usuario ana e ao grupo g-usuarios.

→ Acceso non permitido ao usuario xurxo e ao grupo @g-external. **invalid users prevalece no caso de conflito con valid users**

Acceso permitido á dirección IP 127.0.0.1, á rede 172.16.10.0/24 e ao host lclient1

Acceso non permitido aos host 172.16.10.150 e lclient2

- **hosts allow prevalece no caso de conflito con hosts deny**
- **hosts deny prevalece no caso de conflito con valid users**

No Cliente

usuarios/grupos Samba → que non teñen por que existir no cliente.

```
# mkdir /mnt/descargas
```

```
# mount.cifs //lserver1/descargas /mnt/descargas -o user=ana,uid=1001,gid=1001,file_mode=0777,dir_mode=0777
```

```
# ls -ld /mnt/descargas
```

```
# mkdir /mnt/descargas/dir1-ana && touch /mnt/descargas/f1-ana.txt
```

```
# umount /mnt/descargas
```

```
# mount.cifs //lserver1/descargas /mnt/descargas -o user=xurxo,uid=1001,gid=1001,file_mode=0400,dir_mode=0500
```

```
# usermod -G g-external xurxo
$ id ana && id xurxo
uid=1001(ana) gid=1001(ana) grupos=1001(ana),1003(g-usuarios)
uid=1002(xurxo) gid=1002(xurxo) grupos=1002(xurxo),1004(g-external)
```

O usuario Samba **ana** pode montar o recurso compartido xa que pode autenticar (valid users + hosts allow). No cliente os
→ ficheiros posúen permisos ugo 777 e os directorios 777, aínda que no servidor os permisos destes ficheiros e directorios son os xerados no servidor según a configuración de Samba.

→ Revisar permisos do cartafol /mnt/descargas

→ Ao intentar crear directorio e ficheiros no recurso compartido non se pode debido á directiva Samba **read only=yes**

→ Desmontar recurso compartido

→ O usuario Samba **xurxo** non pode montar o recurso compartido xa que non pode autenticar (invalid users).

No Servidor

```
# ls -ld /srv/descargas
```

 → Revisar permisos do cartafol /srv/descargas

Revisar permisos dentro do cartafol /srv/descargas. Como cando creamos o recurso compartido /srv/descargas executamos o comando **chmod 2770 /srv/descargas**, (SGID 2000), e se a directiva deste recurso compartido no servidor Samba fose *read only = no*, todos os subdirectorios creados en /srv/descargas terán como grupo propietario o grupo propietario do directorio principal /srv/descargas, sendo neste caso o grupo g-usuarios.

```
# ls -l /srv/descargas
```


Exemplo: [homes] → libpam-mount → Montar home no login - Desmontar home no logout

- **libpam-mount** (man pam_mount && man pam_mount.conf)(/etc/security/pam_mount.conf.xml)(~/pam_mount.conf.xml)
- %(USER), %(USERID): Variables pam_mount. Identifican user_samba/uid_user_samba respectivamente. **Non se modifican**
- Para que funcione a compartición → **password_user_system = password_user_samba** → smbpasswd -a user_samba

[homes]

comment = Home Directories → Descrición da sección a visualizar
browseable = no → Este recurso compartido non se amosa ao explorar a rede.
read only = yes → Permisos de só lectura
create mask = 0700 → Máximo nivel de permisos dos ficheiros a crear dentro do cartafol do usuario (u g o = rwx --- ---).
directory mask = 0700 → Controla permisos ugo no lado do servidor.
valid users = %S → Máximo nivel de permisos dos directorios a crear dentro do cartafol do usuario (u g o = rwx --- ---).
→ %S → os usuarios acceden ao seu cartafol persoal:
user_samba → /home/user_samba → \\server\user_samba

No Cliente

pam_mount → os usuarios Samba teñen que existir no cliente como usuarios Unix co mesmo contrasinal de acceso que en Samba, xa que imos montar no login e desmontar no logout.

```
root@lclient1:~# groupadd g-usuarios && usermod -aG g-usuarios usuario
usuario@lclient1:~$ id usuario
uid=1000(usuario) gid=1000(usuario)
grupos=1000(usuario),24(cdrom),25(floppy),29(audio),30(dip),44(video),
46(plugdev),109(netdev),112(blueetooth),116(scanner),119(lpadmin),1001(g-usuarios)
```

```
<!-- Volume definitions -->
<volume sgrp="g-usuarios" fstype="cifs" server="lserver1"
path="homes" mountpoint="/home/%(USER)"
options="nodev,nosuid,workgroup=WORKGROUP" />
```

```
# su - usuario
# mount
# ls -ld /home/usuario
# mkdir /home/usuario/dir1 && touch /home/usuario/f1
# exit
```

Engadir en /etc/security/pam_mount.conf.xml para montar no login o recurso compartido [homes](path). 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 cliente Samba.**
→ Login → passwd pam_mount = passwd user_samba → pam_mount monta volume cifs en /home/usuario
→ Verificar volumes montados.
→ Revisar permisos do cartafol /home/usuario
→ Ao intentar crear directorio e ficheiros no recurso compartido non se pode debido á directiva Samba **read only=yes**
→ Logout → Desmontar recurso compartido

No Servidor

usuario → é un usuario Unix e Samba onde:

- password_user_system = password_user_samba
- Non pertence ao grupo g-usuarios.

```
usuario@lserver1:~$ id usuario
uid=1000(usuario) gid=1000(usuario)
grupos=1000(usuario),24(cdrom),25(floppy),29(audio),30(dip),44(video),
46(plugdev),109(netdev),112(blueetooth),116(scanner),119(lpadmin)
```

[homes] → **read only = no** → Modificar a directiva **read only = no** en /etc/samba/smb.conf na sección [homes]
smbcontrol all reload-config → Recargar a configuración do Servidor Samba

No Cliente

Probar de novo a creación de ficheiros e directorios

Exemplo: Compartir Impresoras → [global] → backend cups → [printers] → impresoras compartidas

- Samba precisa dun servidor de impresión como backend, o cal debe estar instalado localmente no host Samba, xa que Samba non pode reenviar traballos de impresión a un host remoto.
- **cups** → Servidor de impresión empregado como backend no Servidor Samba. Debe estar instalado localmente no servidor Samba
- /var/tmp → Directorio cola impresión Samba (ugo → 1777)
- Na configuración por defecto en /etc/samba/smb.conf todas as impresoras configuradas no backend de impresión (cups) están compartidas automaticamente.

[printers]

comment = All Printers → Descrición da sección a visualizar
browseable = no → Este recurso compartido non se amosa ao explorar a rede.
path = /var/tmp → Accédese ao recurso compartido /var/tmp mediante o nome da sección printers.
printable = yes → Recurso compartido impresora está dispoñible
guest ok = no → Acceso permitido soamente aos usuarios autenticados
read only = yes → Permisos de só lectura
create mask = 0700 → Máximo nivel de permisos dos ficheiros a crear dentro do cartafol definido na directiva path (u g o = rwx --- ---). Controla permisos ugo no lado do servidor.

CUPS (servidor de impresión empregado como backend en Samba)

```
# apt -y install cups  
# apt -y install printer-driver-cups-pdf  
https://localhost:631/printers/PDF
```

→ Instalar cups
→ Instalar **printer-driver-cups-pdf (Impresora virtual PDF)**
Acceder ao panel de Impresoras de cups. Debe existir a impresora virtual de nome PDF
→ **Controlador:** Generic CUPS-PDF Printer (w/ options) (color)
Os arquivos impresos serán gardados no servidor en ~/PDF, é dicir, /home/user_samba/PDF

Samba4 (compartir impresoras mediante backend CUPS)

No Servidor

```
# smbctl -b | grep "HAVE_CUPS"  
HAVE_CUPS_CUPS_H  
HAVE_CUPS_LANGUAGE_H  
HAVE_CUPS  
HAVE_LIBCUPS
```

→ Verificar soporte cups de Samba, é dicir, Samba foi instalado co soporte CUPS habilitado. Se non amosa saída → **instalar Samba con soporte cups**

```
[global] → printing = CUPS  
[PDF]  
path = /var/tmp  
printer = PDF  
comment = Impresora PDF CUPS  
browseable = yes  
write ok = yes  
##valid users = usuario
```

→ Engadir a directiva **printing = CUPS** en /etc/samba/smb.conf na sección **[global]**
→ Engadir a sección **[PDF]** en /etc/samba/smb.conf correspondente á impresora CUPS PDF xerada anteriormente

```
# ls -ld /var/tmp  
# smbcontrol all reload-config
```

→ Revisar permisos do cartafol colas de impresión /var/tmp (ugo → 1777)
→ Recargar a configuración do Servidor Samba

No Cliente

```
# apt -y install cups smbclient
```

```
# echo 172.16.10.254 lserver1 | tee -a /etc/hosts
```

lclient1 → **https://localhost:631/admin** → Añadir impresora → Windows Printer via SAMBA → Conexión: **smb://user_samba:passwd_samba@WORKGROUP/lserver1/PDF** → Nombre: PDF, Descripción: PDF Virtual, Ubicación: lserver1 → Controlador: Generic PostScript Printer(en) → Añadir

Crear archivo e imprimir escollendo a impresora PDF

<https://localhost:631/printers/PDF> → Mantenimiento → Imprimir página de prueba

→ Instalar cups e smbclient

→ Lembrar asignar o nome lserver1 á IP do servidor

Engadir a impresora virtual PDF compartida por Samba → **Controlador:** **PostScript** Generic PostScript Printer[en](recomendado)

Revisar directorio /var/tmp(cola de impresión) do servidor e no caso que no

→ cliente \$HOME esté montado por Samba revisar o cartafol /home/user_samba/PDF

Testar 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 montagem de arrays

sdb1	sdb2	
------	------	--

sdc1	sdc2	
------	------	--

sdd1	sdd2	
------	------	--

sde1	sde2	
------	------	--

RAID5(/dev/md5): 4 discos/partições

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

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

/dev/md0 → /mnt/md0

```
# apt update && apt -y install mdadm parted
# for i in sdb sdc sdd sde
do
    parted -s /dev/${i} print
    parted --script /dev/${i} mklabel msdos
    parted --script /dev/${i} mkpart primary 0 50% -a cylinder
    parted --script /dev/${i} mkpart primary 50% 70% -a cylinder
    parted -s /dev/${i} print
done
# cat /proc/mdstat
# yes | mdadm --create /dev/md5 --level=5 \
--raid-devices=3 /dev/sdb1 /dev/sdc1 /dev/sdd1 \
--spare-devices=1 /dev/sde1
# yes | mdadm --create /dev/md0 --level=0 \
--raid-devices=4 /dev/sdb2 /dev/sdc2 /dev/sdd2 /dev/sde2
# cat /proc/mdstat
# mdadm --examine --scan >> /etc/mdadm/mdadm.conf
# mdadm --detail /dev/md5
# mdadm --detail /dev/md0
# mkdir /mnt/md5 /mnt/md0
# mkfs.ext4 -F -L 'RAID5' /dev/md5
# mkfs.ext4 -F -L 'RAID0' /dev/md0
# UUID_MD5=$(lsblk -o +UUID | grep md5 | awk '{print $NF}' | sort -u)
# echo "UUID=${UUID_MD5} /mnt/md5 ext4 defaults 0 2" >> /etc/fstab
# UUID_MD0=$(lsblk -o +UUID | grep md0 | awk '{print $NF}' | sort -u)
# echo "UUID=${UUID_MD0} /mnt/md0 ext4 defaults 0 2" >> /etc/fstab
# mount -a
# mount || findmnt
# mkdir -p /mnt/md5/dir5 && touch /mnt/md5/dir5/f1
# mkdir -p /mnt/md0/dir0 && touch /mnt/md0/dir0/f0
# ls -lR /mnt/md5 /mnt/md0
# umount /mnt/md5 /mnt/md0
# mount || findmnt
# update-initramfs -u
# reboot
```

```
$ mount || findmnt
$ cat /proc/mdstat
# mdadm --detail /dev/md5
# mdadm --detail /dev/md0
# ls -lR /mnt/md5 /mnt/md0
```

→ Criar os arrays de disco
→ RAID5(/dev/md5)
e
RAID0(/dev/md0)

→ Uma vez iniciado
→ verificar se os arrays estão funcionando

Apéndice. Configuración de rede

Configuración Manual

ip
ifconfig (deprecated)
route (deprecated)
(apt install net-tools)
/etc/resolv.conf
dhclient

```
# ip address show || ip addr show || ip a  
# ifconfig -a
```

→ Comandos equivalentes. Amosar a configuración de rede de todas as NIC estén ou non activas.

```
# ip link set eth0 down && ip link set eth0 up  
# ifconfig eth0 down && ifconfig eth0 up
```

→ Deshabilitar NIC eth0 e Habilitar NIC eth0

```
# ip address add 172.16.10.254/24 dev eth0  
# ifconfig eth0 172.16.10.254/24
```

→ Configuración de rede para a NIC eth0: IP=172.16.10.254, MS=255.255.255.0

```
# ip address del 172.16.10.254/24 dev eth0  
NON EXISTE EQUIVALENCIA CON ifconfig
```

→ Eliminar configuración rede para NIC eth0: IP=172.16.10.254, MS=255.255.255.0

```
# ip route show || ip route list || ip route || ip r  
# route
```

→ Listar táboa de enrutamento

```
# ip route add default via 172.16.10.1  
# route add default gw 172.16.10.1
```

→ Configurar porta de enlace(gateway)

```
# ip route del default via 172.16.10.1  
# route del default gw 172.16.10.1
```

→ Eliminar porta de enlace(gateway)

```
# ip route add 172.16.10.0/24 dev eth0  
# route add -net 172.16.10.0 netmask 255.255.255.0 dev eth0
```

→ Engadir regra de enrutamento para a rede 172.16.10.0 na NIC eth0

```
# ip route del 172.16.10.0/24 dev eth0  
# route del -net 172.16.10.0 netmask 255.255.255.0 dev eth0
```

→ Eliminar regra de enrutamento para a rede 172.16.10.0 na NIC eth0

```
# echo 'domain example.local' > /etc/resolv.conf
```

→ Dominio a engadir na procura de hostnames. Se o host a buscar é host1, é a procura falla, intentárase de novo esta como host1.example.local
Lista de dominios a engadir na procura de hostnames.

```
# echo 'search example.local' > /etc/resolv.conf
```

→ domain e search son excluíntes, a última directiva que apareza no ficheiro prevalece

```
# echo 'nameserver 8.8.8.8' >> /etc/resolv.conf
```

→ Agregar servidor DNS primario para resolución de nomes.

```
# echo 'nameserver 8.8.4.4' >> /etc/resolv.conf
```

→ Agregar servidor DNS secundario para resolución de nomes.

```
# dhclient -v eth0
```

→ Configuración dinámica de rede da NIC eth0 en modo verbose(detallado)

```
# dhclient -s 172.16.16.16 -v eth0
```

→ A diferenza do comando anterior procura a configuración no servidor DHCP 172.16.16.16

Configuración ficheiros networking

/etc/network/interfaces [1] [2]



(man interfaces)

/etc/inid.d/networking [action]

systemctl [action] networking

/etc/resolv.conf

(Ver apartado Conf. Manual)

resolvconf

(man 8 resolvconf)

```
# cat /etc/network/interfaces  
auto lo  
iface lo inet loopback  
auto eth0  
iface eth0 inet static  
address 172.16.10.254  
netmask 255.255.255.0  
gateway 172.16.10.1
```

```
auto eth1  
iface eth1 inet dhcp
```

```
allow-hotplug eth2  
iface eth2 inet dhcp
```

Configuración estática NIC eth0 e dinámica (servidor DHCP) para as NIC eth1 e eth2, onde:

- **auto**: Emprégase para interfaces que sempre están presentes e deséxase que estean activas inmediatamente ao iniciar o sistema.
- **allow-hotplug**: Emprégase para interfaces extraíbles ou que poderían non estar conectadas durante o arranque, pero que se desexa que se configuren automaticamente ao detectarse.

O demo networking é o proceso/demo NetworkManager son excluíntes. Así, debemos asegurarnos que o proceso/demo NetworkManager non estea activo:

```
# pkill NetworkManager || /etc/init.d/network-manager stop || systemctl stop network-manager  
# systemctl disable network-manager && systemctl enable networking
```

```
# /etc/init.d/networking
```

```
Usage: /etc/init.d/networking {start|stop|reload|restart|force-reload}
```

→ Accións do demo networking

```
# /etc/init.d/networking [action] || systemctl [action] networking
```

→ Executar a [action] no demo networking

Configuración ficheiros networking

/etc/network/interfaces [1] [2]



(man interfaces)

/etc/inid.d/networking [action]

systemctl [action] networking

/etc/resolv.conf

(Ver apartado Conf. Manual)

resolvconf

(man 8 resolvconf)

```
# tree -L 1 /etc/network
```

```
/etc/network/  
├── if-down.d  
├── if-post-down.d  
├── if-pre-up.d  
├── if-up.d:  
├── interfaces  
└── interfaces.d
```

```
# ifup eth0  
# ifdown eth0
```



if-down.d → Directorio para scripts que se executarán antes de desactivar as NIC. → [down](#) || [pre-down](#)
if-post-down.d → Directorio para scripts que se executarán logo de desactivar as NIC. → [post-down](#)
if-pre-up.d → Directorio para scripts que se executarán antes de activar as NIC. → [pre-up](#)
if-up.d: → Directorio para scripts que se executarán despois de activar as NIC. → [up](#) || [post-up](#)
Se un script colócase neses directorios, non será executado automaticamente, a menos que sexa referenciado no ficheiro de interfaces dentro dunha estrutura(sección) **iface**, mediante:

- **pre-up**: Acción que se realiza antes de activar a interface.
- **up**:
post-up: Alias de **up**. Acción que se realiza despois de activar a interface.
- **down**
pre-down: Alias de **down**. Acción que se realiza antes de desactivar a interface.
- **post-down**: Acción que se realiza despois de desactivar a interface.

As accións poden ser comandos ou scripts. Se se invocan scripts deben existir senón o servizo networking non arrancará. Para que se executen os scripts é necesario que posúan permisos de execución (chmod +x)

interfaces → Este ficheiro contén a configuración principal das interfaces de rede.

interfaces.d → Neste directorio poden engadirse ficheiros adicionais para organizar a configuración das interfaces de rede de forma modular.

As NIC configuradas con /etc/network/interfaces pódense activar e desactivar con **ifup** e **ifdown** respectivamente.

```
# cat /etc/network/interfaces
```

```
auto lo  
iface lo inet loopback
```

```
auto eth0  
iface eth0 inet static  
    address 172.16.10.254/24  
    gateway 172.16.10.1  
    post-up /etc/network/if-up.d/add_route_network.sh  
    pre-down /etc/network/if-down.d/del_route_network.sh  
    dns-nameservers 8.8.4.4 8.8.8.8  
    dns-search ies.local
```

```
# cat /etc/network/if-up.d/add_route_network.sh  
route add -net 10.10.10.0 netmask 255.255.255.0 gw 172.16.10.1
```

```
# cat /etc/network/if-down.d/del_route_network.sh  
route add -net 10.10.10.0 netmask 255.255.255.0 gw 172.16.10.1
```



Configuración estática NIC eth0, onde:

- **address**: Permite definir a dirección IP e Máscara de Subrede en formato CIDR sen ter que empregar a directiva netmask
- **gateway**: Porta de enlace
- **post-up**: Despois de activar eth0 executa o script [add_route_network.sh](#)
- **pre-down**: Antes de desactivar eth0 executa o script [del_route_network.sh](#)
- **dns-nameservers**: Definir os servidores DNS para eth0: 8.8.4.4 como primario e 8.8.8.8 como secundario. Para que funcione ten que estar instalado o paquete [resolvconf](#), de tal xeito que ao recargar esa configuración co [demo networking](#), [resolvconf](#) modificará o arquivo [/etc/resolv.conf](#) con esta configuración.
- **dns-search**: Definir a directiva [search](#) para eth0. Para que funcione ten que estar instalado o paquete [resolvconf](#), de tal xeito que ao recargar esa configuración co [demo networking](#), [resolvconf](#) modificará o arquivo [/etc/resolv.conf](#) con esta configuración.