Servei SAMBA (part2)
Administració Avançada

Curs 2016-2017

Descripció dels aprenentatges:

Bàsic

1. Instal·lar el servei samba.
2. Configuració bàsica de shares.
3. Eines samba clients.
4. Gestió D'usuaris.
5. Permisos d'usuaris als shares.
6. Configuració i procés d'elecció del Master Browser.
7. Rols.

Intermig

8. Password Backend amb ldapsam.
9. Dominis amb validació d'usuaris PDC i Domain Members (netlogons)
10. Integració d'equips heterogenis Unix, GNU/Linux i Windows.

Avançat

11. Samba i PAM
12. Samba amb LDAP i Kerberos

Documentació

LLibre Samba O'Reilly: Using Samba, 2ed, O'Reilly & Associates (Feb. 2003)

- **1. Learning the Samba**
- **2. Installing Samba on a Unix System**
- **3. Configuring Windows Clients**
- **4. Windows NT Domains**
- **5. Unix Clients**
- **6. The Samba Configuration File**
- **7. Name Resolution and Browsing**
- **8. Advanced Disk Shares**
- **9. Users and Security**
- **10. Printing**
- **11. Additional Samba Information**
- **Appendix A. Example Configuration Files**
- **Appendix B. Samba Configuration Option Quick Reference**
- **Appendix E. Configure Options**

Referències

- Pàgines man
- http://docs.fedoraproject.org/en-US/Fedora/15/html/Deployment_Guide/ch-File_and_Print_Servers.html#s1-Samba
- http://trauko.wordpress.com/2007/09/17/instalando-samba-en-ubuntu-para-compartir-archivos-e-impresoras-en-redes-windows/
- http://samba.org/samba/docs/using_samba/toc.html
- http://samba.org/samba/docs/man/Samba-Guide/
- http://samba.org/samba/docs/man/Samba-HOWTO-Collection/
- http://download.gna.org/smbldap-tools/docs/

Global Configuration

Opcions de configuració:

- **netbios name**: nom del servidor (NO fqdn del DNS o nom arbitrari del server)
- **workgroup**: nom del grup de treball o del domini (segons sigui standalone o PDC). Es en realitat un NetBios group.Els host han de pertànyer al mateix workgrup/domain per compartir recursos samba.
- **server string**: descripció del servidor samba

Tipus de rol:

- **server standalone**: un host 'windows' que pertany a un grup-de-treball/domain de manera stand-alone. No hi ha cap controlador de domini, són hosts que comparteixen recursos entre ells. Xarxa peer-to-peer.
- **PDC Controlador de domini**: un server que controla un domini/grup-de-treball. És qui autentifica els usuaris i gestiona els recursos del domni. Xarxa client-servidor.
- **master browser**: en un entorn de grup-de-treball un dels servers es pot erigir en master-browser i ser qui gestiona la llista d'integrants del grup-de-treball. En un domini el PDC realitza aquesta funció.
- **BDC**: controlador secundari de domini.

Resolució de noms windows: nmb

- **wins support = yes** el host realitza la resolució de noms windows. És el servidor de noms windows (com un dns per a noms de windows)
- **wins support = no** el host fa de client wins, és a dir, per identificar els noms dels altres hosts ho ha de demanar al servidor de noms wins.

Opcions de un recurs compartit: SHARES

- path /path/to/share
- comment "comment"
- volume "name"
- read only yes/no
- writtable yes/no

Shares: recursos de disc i d'impressió

El model SAMBA Client/Server de Shares

Com és sabut podem generar recursos compartits en una xarxa anomenats ***Shares***. Aquests recursos en el nivell bàsic poden ser:

- De **disc**.
- D'**impressió**.

Qui pot generar aquests recursos? De fet qualsevol sistema operatiu Windows pot generar recursos compartits (des de hosts windows fins a servidors Windows) amb la coneguda opció "*compartir com*". però també equips GNU/Linux utilitzant SAMBA poden oferir recursos de disc i d'impressió a altres hosts.

Així doncs, podem tenir:

- Un host **Windows** que ofereix recursos de xarxa o Shares. Els seus clients poden ser altres Windows o GNU/Linux que utilitzen clients de SAMBA.
- Un host **GNU/Linux** que ofereix recursos de xarxa usant el protocol SAMBA. Els seus clients poden ser tant equips Windows com altres GNU/Linux que executen el software de SAMBA client.

El software de SAMBA (a nivell bàsic) pot actuar com a:

- **Client** de recursos o *Shares* d'equips que els ofereixen a la xarxa (siguin equips Windows o GNU/Linux). per exemple les ordres smbclient, smbget, mount.cifs, etc.
- **Servidor** de recursos de xarxa, Shares, als que es poden connectar altres equips siguin Windows o GNU/Linux.

SAMBA proporciona més funcionalitats (avançades) per implementar des d'equips GNU/Linux l'administració de xarxes Windows. permet:

- Actuar com a **browser** de la xarxa.
- Actuar com a servidor **WINS** de la xarxa.
- Actuar com a Server Member d'una xarxa Windows.
- Actuar com a PDC o Controlador principal de Domini d'una xarxa Windows.

El protocol SAMBA/SMB/CIFS

SMB: El protocol Windows per a la gestió de recursos de disc i d'impressores en xarxa, per a fer '*compartir com*' i '*conectar a unidad de red*' és el protocol SMB Server Message Block.

SAMBA: El software *opensource* que permet implementar el protocol SMB en equips GNU/LInux s'anomena SAMBA, fent un joc de paraules amb la pronúncia del protocol de Windows SMB.

CIFS: Windows va evolucionar el seu protocol de compartició de recursos de disc al protocol actualment anomenat CIFS Common internet File System. Des del punt de vista d'aquesta documentació SMB i CIFS realitzen la mateixa funció.

Crear Shares des de hosts windows

Uzn equip Windows (en totes les seves versions) permet compartir '**carpetes**' i **impressores**. És la opció "*compartir com*". Un cop compartides altres hosts es poden connectar aquests recursos.
Segons la versió de Windows utilitzada o les preferències de l'usuari/administrador els recursos es poden compartir usant dos models de seguretat diferents.

Seguretat d'accés:

- Per **recurs**: (Share Level Access Control) permet compartir un recurs amb seguretat a nivell de recurs que únicament permet:
    - Accés públic al recurs sense cap tipus de seguretat.
    - Indicar un *password (generic)* per restringir l'accés al recurs. Els clients que indiquen el password correctament poden accedir al recurs, els altres no.
    - Indicar-se si és *read/write* o només *read only*.
    - A tot recurs se li assigna un nom de recurs, que no té perquè coincidir amb el nom real.
    - També se li pot assignar un comentari descriptiu del recurs.
- Per **usuari**: (User Level Access Control) més avançat i complert. Permet establir una *ACL* o llista de control d'accés indicant quins usuaris/grups poden fer què en el recurs. La granularitat en atorgar permisos és més detallada. Cal indicar:
    - Nom del recurs compartit.
    - Descripció (optativa) del recurs).
    - Llista d'usuaris/grups i permisos assignats en cada cas (una ACL).

- Els recursos es poden fer **públics** (o *browseables*) o poden ser **ocults**. Aquells recursos que comencen amb el *caràcter $* en el seu nom són ocults.
- Segons la versió de Windows també es pot indicar el número màxim de connexions permeses al recurs.
- Les opcions concretes varien en funció de la versió de sistema operatiu Windows utilitzat.

Connectar a shares des de hosts windows

Des dels equips Windows actuar com a client de recursos de xarxa o *Shares* simplement cal seleccionar "**connectar a unitat de xarxa**" i indicar el UNC corresponent.

Usualment els clients Windows proporcionen la facilitat d'assignar un nom de **lletra d'unitat** a un recurs de disc, així per exemple *H:* pot estar assignada a *//server/recurs*.

Unix Clients amb SAMBA

Documentation: Samba Documentation Chapter 5 Unix Clients

Les principals utilitats GNU/Linux clients de SAMBA son:

- smbtree
- smbclient
- smbget
- mount.cifs

Altres ordres: smbcacls, smbclient4, smbcontrol, smbcquotas, smbget, smbpasswd, smbspool, smbtar i smbta-util.

També podem accedir a recursos SAMBA utilitzant eines de l'entorn gràfic com per exemple:

- Un **navegador**, per exemple *firefox*.
- Un browser de fitxers com per exemple **nautilus**.

```
[root@hp01 ~]# docker run ...

[root@hp01 ~]# docker start  -a cont-samba02
[root@2ea1ac403693 ~]# /usr/sbin/smbd
[root@2ea1ac403693 ~]# /usr/sbin/nmbd

[root@2ea1ac403693 ~]# smbtree
Enter GUEST's password:
MYGROUP
    \\2EA1AC403693              Samba Server Version 4.2.3
        \\2EA1AC403693\IPC$                 IPC Service (Samba Server Version 4.2.3)
        \\2EA1AC403693\public               Share de contingut public
        \\2EA1AC403693\manpages             Documentacio man del container
        \\2EA1AC403693\documentation        Documentaciódoc del container

[root@2ea1ac403693 ~]# smbclient -L 2EA1AC403693
Enter GUEST's password:
```

```
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
   Sharename       Type      Comment
   ---------       ----      -------
   documentation   Disk      Documentació doc del container
   manpages        Disk      Documentació man del container
   public          Disk      Share de contingut public
   IPC$            IPC       IPC Service (Samba Server Version 4.2.3)
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
   Server               Comment
   ---------            -------
   2EA1AC403693         Samba Server Version 4.2.3
   Workgroup            Master
   ---------            -------
   MYGROUP              2EA1AC403693
```

```
[root@hp01 ~]# docker inspect cont-samba02 | grep "IPAddress"
        "IPAddress": "172.17.0.3",

[ecanet@hp01 ~]$ smbtree
Enter ecanet's password:
MYGROUP
   \\2EA1AC403693              Samba Server Version 4.2.3
        \\2EA1AC403693\IPC$                IPC Service (Samba Server Version 4.2.3)
        \\2EA1AC403693\public              Share de contingut public
        \\2EA1AC403693\manpages            Documentació man del container
        \\2EA1AC403693\documentation       Documentació doc del container

[ecanet@hp01 ~]$ smbclient -L \\172.17.0.3
Enter ecanet's password:
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
   Sharename       Type      Comment
   ---------       ----      -------
   documentation   Disk      Documentacióddoc del container
   manpages        Disk      Documentacio man del container
   public          Disk      Share de contingut public
   IPC$            IPC       IPC Service (Samba Server Version 4.2.3)
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
   Server               Comment
   ---------            -------
   2EA1AC403693         Samba Server Version 4.2.3
   Workgroup            Master
   ---------            -------
```

```
MYGROUP          2EA1AC403693
```

smbclient

Estudiar l'ordre *smbclient* analitzant els casos següents:

- Usuari actual de la sessió GNU/Linux.
- Usuari anònim.
- Usuari identificat.
- Sessió interactiva
- Sessió desatesa.
- Realitzar còpies de backup.

```
[ecanet@hp01 ~]$ smbclient  //2EA1AC403693/documentation
Enter ecanet's password:  <enter>
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
smb: \> pwd
Current directory is \\2EA1AC403693\documentation\
smb: \> quit

[ecanet@hp01 ~]$ smbclient -N  //2EA1AC403693/manpages
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
smb: \> pwd
Current directory is \\2EA1AC403693\manpages\
smb: \> quit

[ecanet@hp01 ~]$ smbclient -N  //2EA1AC403693/manpages -U userx
Enter userx's password:  <passwd>
userx login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
smb: \> pwd
Current directory is \\2EA1AC403693\manpages\
smb: \> quit
```

smbtree

```
[ecanet@hp01 ~]$ smbtree -D
Enter ecanet's password:
MYGROUP
```

```
[ecanet@hp01 ~]$ smbtree -S
Enter ecanet's password:
MYGROUP
   \\2EA1AC403693              Samba Server Version 4.2.3

[ecanet@hp01 ~]$ smbtree
Enter ecanet's password:
MYGROUP
   \\2EA1AC403693              Samba Server Version 4.2.3
         \\2EA1AC403693\IPC$                IPC Service (Samba Server Version 4.2.3)
         \\2EA1AC403693\public              Share de contingut public
         \\2EA1AC403693\manpages                  Documentacio man del container
         \\2EA1AC403693\documentation       Documentaciódoc del container
```

smbget

```
[ecanet@hp01 ~]$ smbget smb://2EA1AC403693/public/README.md
Username for public at 2EA1AC403693 [guest]
Password for public at 2EA1AC403693:
Using workgroup MYGROUP, guest user
smb://2EA1AC403693/public/README.md
Downloaded 141b in 4 seconds

[ecanet@hp01 tmp]$ smbget -R smb://2EA1AC403693/documentation/samba
Username for documentation at 2EA1AC403693 [guest]
Password for documentation at 2EA1AC403693:
Using workgroup MYGROUP, guest user
smb://2EA1AC403693/documentation/samba/WHATSNEW.txt
….
smb://2EA1AC403693/documentation/samba/README
Downloaded 327,78kB in 4 seconds
```

mount.cifs

```
[root@hp01 ~]# mount -t cifs -o guest //172.17.0.3/documentation /mnt

[root@hp01 ~]# mount -t cifs
//172.17.0.3/documentation on /mnt type cifs
(rw,relatime,vers=1.0,cache=strict,domain=2EA1AC403693,uid=0,noforceuid,gid=0,noforcegi
d,addr=172.17.0.3,unix,posixpaths,serverino,mapposix,acl,rsize=1048576,wsize=65536,actim
eo=1)
```

```
[root@hp01 ~]# umount /mnt
```

```
[root@hp01 ~]# vim /etc/fstab
//172.17.0.3/manpages   /mnt       cifs       defaults,guest,noauto   0 0

[root@hp01 ~]# mount -a
[root@hp01 ~]# mount /mnt/
[root@hp01 ~]# mount -t cifs
//172.17.0.3/manpages on /mnt type cifs
(rw,relatime,vers=1.0,cache=strict,domain=2EA1AC403693,uid=0,noforceuid,gid=0,noforcegi
d,addr=172.17.0.3,unix,posixpaths,serverino,mapposix,acl,rsize=1048576,wsize=65536,actim
eo=1)
```

Nota Observeu que mentre les ordres smbxxx funcionen indicant el nom de servidor (que es resol usant samba) les ordres unix mount NO són capaces de resoldre aquest nom, i hem de usar la adreça IP (o definir el nom al /etc/hosts).

firefox (deprectated)

Provar les següents *locations* en el navegador local, per exemple *firefox*:

```
smb://
smb://mygroup
smb://172.17.0.3
smb://2EA1AC403693
smb://2EA1AC403693/public
smb://2EA1AC403693/manpages
```

nautilus

Provar les següents *locations* en el *file browser*, per exemple *nautilus*:

```
smb://
smb://mygroup
smb://172.17.0.3
smb://2EA1AC403693
smb://2EA1AC403693/public
smb://2EA1AC403693/manpages
```

Atenció a la de recursos que deixa connectats a la barra esquerra de l'arbre de disc. Podeu navegar també via **Navega per la xarxa** i anar seleccionant els elements.

Unix Server amb SAMBA

Documentació: Samba Chapter 6 The Samba Configuration File

Exemple de configuració Server Shares

En aquest exemple el servidor samba es configura per a:

- Actuar com a simple host que ofereix shares a la xarxa.
- Ofereix els recursos de disc de:
    - documentation (/usr/share/doc) només per a lectura
    - manpages (/usr/share/man) només de lectura.
    - public (/var/lib/samba/public) read/write per a tothom.
    - privat (/var/lib/samba/privat) que no es mostra en els llistats.

- Observar del fitxer de configuració els tres blocs:
    - Global: amb la descripció general del servidor SAMBA.
    - *Shares* homes i printer (estàndard).
    - *Shares* definits per l'administrador.

Configuració del fitxer */etc/samba/smb.conf*:

```
[global]
        workgroup = MYGROUP
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        security = user
        passdb backend = tdbsam
        load printers = yes
        cups options = raw
```

```
[homes]
        comment = Home Directories
        browseable = no
        writable = yes
;       valid users = %S
;       valid users = MYDOMAIN\%S
[printers]
        comment = All Printers
        path = /var/spool/samba
        browseable = no
        guest ok = no
        writable = no
        printable = yes
```

```
[documentation]
        comment = Documentació doc del container
        path = /usr/share/doc
        public = yes
        browseable = yes
        writable = no
        printable = no
        guest ok = yes
[manpages]
        comment = Documentació man  del container
        path = /usr/share/man
        public = yes
        browseable = yes
        writable = no
        printable = no
        guest ok = yes
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        public = yes
        browseable = yes
        writable = yes
        printable = no
        guest ok = yes
[privat]
        comment = Share d'accés privat
        path = /var/lib/samba/privat
        public = no
        browseable = no
        writable = yes
        printable = no
        guest ok = yes
```

Instal·lació (under construction!)

Paquets samba samba-common samba-common-utils
Serveis: smbd, nmbd
No cal reiniciar el servei en fer modificacions a la configuració.
Un dimoni smbd per a cada recurs.
utilitat testparm per verificar la configuració /etc/samba/smb.conf.

Users / Groups (share options) Security

Users / Groups

Als shares es poden establir requisits d'accés segons l'usuari. Samba usa una base de dades pròpia (*tdbsam*) d'usuaris, **aquests usuaris ha d'existir en el sistema unix per poder fer el corresponent mapping** en l'accés a disc. Les ordres *smbpasswd* i *pdbedit* permet treballar amb la base de dades d'usuaris de samba.

Llistat d'opcions de configuració de shares: (taula 9.1 Using Samba)

```
path = /dir1/dir2/share
comment = share description
volume = share name
browseable = yes/no
max connections = #

public = yes/no
guest ok = yes/no
guest account = unix-useraccount
guest only = yes/no

valid users = user1 user2  @group1 @group2 …
invalid users = user1 user2  @group1 @group2 …
auto services = user1 user2  @group1 @group2 …
admin users = user1 user2  @group1 @group2 …

writable = yes/no
read only = yes/no
write list = user1 user2  @group1 @group2 …
read list = user1 user2  @group1 @group2 …

create mode = 0660
directory mode = 0770
```

```
[dave]
        path = /home/dave
        comment = Dave's home directory
        writable = yes
        valid users = dave
```

```
[accounting]
```

```
   comment = Accounting Department Directory
   writable = yes
   valid users = @account
   path = /home/samba/accounting
   create mode = 0660
   directory mode = 0770
```

```
# mkdir /home/samba/accounting
# chgrp account /home/samba/accounting
# chmod 770 /home/samba/accounting
```

```
[global]
   invalid users = root bin daemon adm sync shutdown halt mail news uucp operator
   auto services = dave peter bob

[homes]
   browsable = no
   writable = yes

[sales]
       path = /home/sales
       comment = Sedona Real Estate Sales Data
       writable = yes
       valid users = sofie shelby adilia
       admin users = mike

[salesbis]
       path = /home/sales
       comment = Sedona Real Estate Sales Data
       read only = yes
       write list = sofie shelby
```

smbpasswd

Per crear els usuaris samba (locals) aquests es bases en els usuaris Linux, **que han d'existir**. Cal llavors crear per a cada usuari un compte samba amb l'ordre smbpasswd. Genera en un fitxer propi les parelles nom / passwd de cada usuari samba vàlid.

El següent exemple mostra com crear quatre usuaris super3!. Tot seguit mostra diferents formes d'accés al recurs documentation:

- connecta amb l'usuari unix utilitzat en el client.
- connecta com a usuari anònim: guest
- connecta com a usuària lila i demana el password interactivament
- connecta com a usuària lila amb el password indicat en la línia de comandes.

```
server# smbpasswd -a lila
server# smbpasswd -a patipla
server# smbpasswd -a rock
server# smbpasswd -a pla

client$ smbclient //host01/documentation
client$ smbclient -N //host01/documentation
client$ smbclient //host01/documentation -U lila
client$ smbclient //host01/lila -U lila%smblila
```

Amb ***pdbedit*** podem llistar els usuaris samba:

```
[root@samba docker]# pdbedit -L
patipla:1000:
roc:1002:
lila:1001:
pla:1003:
```

Si volem veure TOTES les dades dels comptes samba locals:

```
[root@samba docker]# pdbedit -vL
---------------
Unix username:      patipla
NT username:
Account Flags:      [U          ]
User SID:           S-1-5-21-82721356-3175886355-667739105-1000
Primary Group SID: S-1-5-21-82721356-3175886355-667739105-513
Full Name:
Home Directory:     \\samba\patipla
HomeDir Drive:
Logon Script:
Profile Path:       \\samba\patipla\profile
Domain:             SAMBA
Account desc:
Workstations:
Munged dial:
Logon time:         0
Logoff time:        Wed, 06 Feb 2036 15:06:39 UTC
Kickoff time:       Wed, 06 Feb 2036 15:06:39 UTC
Password last set:  Fri, 14 Dec 2018 11:33:40 UTC
Password can change:  Fri, 14 Dec 2018 11:33:40 UTC
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
---------------
Unix username:      roc
NT username:
Account Flags:      [U          ]
User SID:           S-1-5-21-82721356-3175886355-667739105-1002
Primary Group SID: S-1-5-21-82721356-3175886355-667739105-513
Full Name:
```

```
Home Directory:      \\samba\roc
HomeDir Drive:
Logon Script:
Profile Path:        \\samba\roc\profile
Domain:              SAMBA
Account desc:
Workstations:
Munged dial:
Logon time:          0
Logoff time:         Wed, 06 Feb 2036 15:06:39 UTC
Kickoff time:        Wed, 06 Feb 2036 15:06:39 UTC
Password last set:   Fri, 14 Dec 2018 11:33:41 UTC
Password can change:  Fri, 14 Dec 2018 11:33:41 UTC
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours          : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
---------------
Unix username:       lila
NT username:
Account Flags:       [U          ]
User SID:            S-1-5-21-82721356-3175886355-667739105-1001
Primary Group SID: S-1-5-21-82721356-3175886355-667739105-513
Full Name:
Home Directory:      \\samba\lila
HomeDir Drive:
Logon Script:
Profile Path:        \\samba\lila\profile
Domain:              SAMBA
Account desc:
Workstations:
Munged dial:
Logon time:          0
Logoff time:         Wed, 06 Feb 2036 15:06:39 UTC
Kickoff time:        Wed, 06 Feb 2036 15:06:39 UTC
Password last set:   Fri, 14 Dec 2018 11:33:41 UTC
Password can change:  Fri, 14 Dec 2018 11:33:41 UTC
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours          : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
---------------
Unix username:       pla
NT username:
Account Flags:       [U          ]
User SID:            S-1-5-21-82721356-3175886355-667739105-1003
Primary Group SID: S-1-5-21-82721356-3175886355-667739105-513
Full Name:
Home Directory:      \\samba\pla
HomeDir Drive:
Logon Script:
Profile Path:        \\samba\pla\profile
Domain:              SAMBA
Account desc:
Workstations:
Munged dial:
Logon time:          0
Logoff time:         Wed, 06 Feb 2036 15:06:39 UTC
Kickoff time:        Wed, 06 Feb 2036 15:06:39 UTC
Password last set:   Fri, 14 Dec 2018 11:33:41 UTC
Password can change:  Fri, 14 Dec 2018 11:33:41 UTC
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours          : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Exemples de validació d'usuaris

Trick amb l'ordre testparm podeu verificar o observar quines de les directives de configuració dels shares estan actualment definides.

Usem la següent configuració global:

```
[global]
        workgroup = MYGROUP
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        security = user
        passdb backend = tdbsam
        load printers = yes
        cups options = raw
```

Exemple 1: Usuari guest fa idmap a nobody

guest ok = yes
Permet l'accés al share de usuaris anònims, sense identificar. és equivalent a la opció *public = yes*
Observar que l'accés a disc de l'usuari anònim guest es transforma (id mapping) en l'usuari unix ***nobody***.

```
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        browseable = yes
        writable = yes
        guest ok = yes
```

```
[ecanet@d02 samba:18users]$ smbclient -N //samba/public
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> get README.md
getting file \README.md of size 1900 as README.md (59.9 KiloBytes/sec) (average 59.9
KiloBytes/sec)
smb: \> put README.md red2.txt
putting file README.md as \red2.txt (927.7 kb/s) (average 927.7 kb/s)
smb: \> q
```

```
[root@samba docker]# ll /var/lib/samba/public/
-rw-r--r--. 1 root   root  375 Dec 14 11:27 Dockerfile
-rw-r--r--. 1 root   root   1900 Dec 14 11:27 README.md
-rwxr--r--. 1 nobody nobody 1900 Dec 14 11:36 red2.txt
```

Exemple 2: Només usuari guest

guest only = yes

Permet únicament accedir al recurs via usuari anònim. No es permet l'accés via usuari identificat.

Observem que el sistema ens enganya, ens diu que ens deixa entrar com l'usuari *lila* però en realitat som *nobody*.

```
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        browseable = yes
        writable = yes
        printable = no
        guest only = yes
```

```
[ecanet@d02 samba:18users]$ smbclient -U lila  //samba/public
Enter SAMBA\lila's password:
Try "help" to get a list of possible commands.
smb: \> get README.md
getting file \README.md of size 1900 as README.md (1855.3 KiloBytes/sec) (average
1855.5 KiloBytes/sec)
smb: \> put README.md red3.txt
putting file README.md as \red3.txt (927.7 kb/s) (average 927.7 kb/s)
smb: \>
```

```
[root@samba docker]# ll /var/lib/samba/public/
-rw-r--r--. 1 root   root  375 Dec 14 11:27 Dockerfile
-rw-r--r--. 1 root   root   1900 Dec 14 11:27 README.md
-rwxr--r--. 1 nobody nobody 1900 Dec 14 11:43 red3.txt
```

Exemple 3: Usuari només guest amb idmap a un compte unix (deprecated guest account?)

```
[public]
        comment = Share de contingut public
```

```
        path = /var/lib/samba/public
        browseable = yes
        writable = yes
        guest ok = yes
        guest account = pla
```

```
[ecanet@d02 samba:18users]$ smbclient -N  //samba/public
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> get README.md
getting file \README.md of size 1900 as README.md (1855.3 KiloBytes/sec) (average
1855.5 KiloBytes/sec)
smb: \> put README.md red4.txt
putting file README.md as \red4.txt (927.7 kb/s) (average 927.7 kb/s)
smb: \>
```

```
```

Exemple 4: Usuari identificat

Les ordres client samba permeten indicar en nom de quin usuari es vol realitzar la connexió. El password es pot demanar interactivament o indicar-lo en la línia de comanda. Així per exemple amb la ordre smbclient podem fer:

```
$ smbclient -U user //server/recurs
$ smbclient -U user%password //server/recurs
```

```
[ecanet@d02 samba:18users]$ smbclient -U lila  //samba/public
Enter SAMBA\lila's password:
Try "help" to get a list of possible commands.
smb: \> get README.md
getting file \README.md of size 1900 as README.md (927.7 KiloBytes/sec) (average 927.7
KiloBytes/sec)
smb: \> put README.md red5.txt
putting file README.md as \red5.txt (927.7 kb/s) (average 927.7 kb/s)
smb: \>
```

```
[root@samba docker]# ll /var/lib/samba/public/
-rw-r--r--. 1 root   root  375 Dec 14 11:27 Dockerfile
-rw-r--r--. 1 root   root   1900 Dec 14 11:27 README.md
-rwxr--r--. 1 lila   lila   1900 Dec 14 11:49 red5.txt
```

Exemple 5: Valid users

valid users = user1 user2 userN

Permet indicar la llista d'usuaris vàlids per accedir al recurs. La resta d'usuaris no podran accedir-hi. Tampoc guest tot i que s'hagi indicat guest ok.

```
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        browseable = yes
        writable = yes
        guest ok = yes
        valid users = patipla roc
```

```
[ecanet@d02 samba:18users]$ smbclient -N  //samba/public
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

[ecanet@d02 samba:18users]$ smbclient -U lila  //samba/public
Enter SAMBA\lila's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

[ecanet@d02 samba:18users]$ smbclient -U patipla  //samba/public
Enter SAMBA\patipla's password:
Try "help" to get a list of possible commands.
smb: \>

[root@hostedt tmp]# smbclient -U roc%roc //samba/public
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \>
```

Exemple 6: Invalid users

invalid users = user1 user2 userN

Indica la llista d'usuaris que no tenen permès accedir al recurs. La resta d'usuaris vàlids si hi poden accedir (guest dependrà de si s¡ha permès o no via guest ok).

```
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        browseable = yes
        writable = yes
        guest ok = yes
        invalid users = patipla roc
```

```
[ecanet@d02 samba:18users]$ smbclient -N  //samba/public
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>

[ecanet@d02 samba:18users]$ smbclient -U lila  //samba/public
Enter SAMBA\lila's password:
Try "help" to get a list of possible commands.
smb: \>

[ecanet@d02 samba:18users]$ smbclient -U patipla  //samba/public
Enter SAMBA\patipla's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

Exemple 7: Admin users

admin users = user1 user2 userN

Permet defiinir un conjunt d'usuaris samba que seran convertits (id mapping) a l'usuari root. És a dir, estem dient que tal i tal usuari samba quan accedeixi a disc al recurs ha d'actuar com a usuari administrador (root en cas de unix).

```
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        writable = yes
        guest ok = yes
        admin users = roc
```

```
[root@hostedt tmp]# smbclient -U roc%roc //samba/public
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> get README.md
getting file \README.md of size 1900 as README.md (927,7 KiloBytes/sec) (average 927,7 KiloBytes/sec)
smb: \> put README.md file1.pdf
putting file README.md as \file1.pdf (1855,3 kb/s) (average 1855,5 kb/s)
smb: \>
```

```
[root@samba docker]# ll /var/lib/samba/public/
-rw-r--r--. 1 root root 1900 Dec 14 15:44 README.md
-rwxr--r--. 1 root roc  1900 Dec 14 15:52 file1.pdf
```

Exemples de lectura / escriptura / mode

Els recursos es poden configurar de només lectura o de lectura/escriptura. Es pot indicar una llista explícita de qui pot llegir i de qui pot escriure. També es poden indicar els permisos (mode) dels fitxers.

Exemple 8: Recurs de només lectura

read only = yes
writable = no
Els recursos es poden configurar per ser de només lectura (són equivalents).

Exemple 9: Recurs de lectura/escriptura

read only = no
writable = yes
Recursos configurats de lectura/escriptura. Són equivalents.

Exemple 10: Llista d'usuaris autoritzats de lectura

read list = user1 user2 userN
Indica la llista d'usuaris que només poden llegir. Atenció, aquesta directiva s'indica en recursos que són de lectura/escriptura i serveix per restringir aquests usuaris atorgant-los només el dret de lectura (i privant-los del de escriptura)

```
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        writable = yes
        guest ok = yes
        read list = pla
```

```
[root@hostedt tmp]# smbclient -U roc%roc //samba/public
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> ls
  .                   D        0  Fri Dec 14 17:31:06 2018
  ..                  D        0  Fri Dec 14 16:45:31 2018
  file3.txt           A     1900  Fri Dec 14 17:31:06 2018

        10474496 blocks of size 1024. 9892316 blocks available
```

```
smb: \> rm file3.txt
smb: \>

[root@hostedt tmp]# smbclient -U lila //samba/public
Enter lila's password:
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> put README.md file1.txt
putting file README.md as \file1.txt (927,7 kb/s) (average 927,7 kb/s)
smb: \>

[root@hostedt tmp]# smbclient -U pla //samba/public
Enter pla's password:
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> ls
  .                   D        0  Fri Dec 14 17:44:09 2018
  ..                  D        0  Fri Dec 14 16:45:31 2018
  file3.txt           A     1900  Fri Dec 14 17:44:09 2018
        10474496 blocks of size 1024. 9892312 blocks available
smb: \> rm file3.txt
NT_STATUS_MEDIA_WRITE_PROTECTED deleting remote file \file3.txt
NT_STATUS_MEDIA_WRITE_PROTECTED listing \file3.txt
smb: \>
smb: \> put README.md file4.txt
NT_STATUS_ACCESS_DENIED opening remote file \file4.txt
smb: \>
```

Exemple 11: Llista d'usuaris autoritzats per a escriptura

write list = user1 user2 userN

Indica la llista d'usuaris amb dret d'escriptura al recurs. S'utilitza en recursos que són *read only* per a tots els usuaris però es permet als usuaris indicats a la llista el dret de escriptura.

```
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        writable = no
        guest ok = yes
        write list = pla
```

```
[root@hostedt tmp]# smbclient -U lila%lila //samba/public
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> rm file1.pdf
NT_STATUS_MEDIA_WRITE_PROTECTED deleting remote file \file1.pdf
```

```
NT_STATUS_MEDIA_WRITE_PROTECTED listing \file1.pdf
smb: \>

[root@hostedt tmp]# smbclient -U pla //samba/public
Enter pla's password:
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> rm file1.pdf
smb: \> put README.md file1.pdf
putting file README.md as \file1.pdf (1855,3 kb/s) (average 1855,5 kb/s)
smb: \>
```

Exemple 12: Modes de directori i fitxer

create mode = mode
directory mode = mode
Permeten establir el mode dels directoris i els fitxers de nova creació dins el share. (!!!)

```
[root@samba docker]# ll /var/lib/samba/public/
-rwxr--r--. 1 pla           pla       1900 Dec 14 16:53 file1.pdf
-rwxr--r--. 1 lila   lila   1900 Dec 14 16:42 file1.txt
-rwxr--r--. 1 nobody nobody 1900 Dec 14 16:28 file2.txt
-rwxr--r--. 1 nobody nobody 1900 Dec 14 16:44 file3.txt
```

```
[public]
        comment = Share de contingut public
        path = /var/lib/samba/public
        writable = yes
        guest ok = yes
        create mask = 0600
        directory mask = 0700
```

```
[root@hostedt tmp]# smbclient -U roc%roc //samba/public
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> mkdir newdir
smb: \> put README.md newfile.txt
putting file README.md as \newfile.txt (1855,3 kb/s) (average 1855,5 kb/s)
smb: \>
```

```
[root@samba docker]# ll /var/lib/samba/public/
-rwxr--r--. 1 lila   lila   1900 Dec 14 16:42 file1.txt
-rwxr--r--. 1 nobody nobody 1900 Dec 14 16:28 file2.txt
-rwxr--r--. 1 nobody nobody 1900 Dec 14 16:44 file3.txt
drwx------. 2 roc           roc          6 Dec 14 17:03 newdir
```

```
-rw-------. 1 rocroc      1900 Dec 14 17:04 newfile.txt
```

Security

Nivells de seguretat/autenticació:

- Share-level security. (deprecated)
- User-level security.
- Server-level security. (deprecated)
- Domain-level security.

```
[global]
        security = share
[data]
        username = andy, peter, terry
```

```
[global]
        security = user

[accounting1]
        writable = yes
        valid users = bob, joe, sandy
```

```
[global]
        security = server
        password server = mixtec toltec
```

Al llarg del temps windows ha anat usant diversos modes de seguretat, alguns d'ells actualment deprecated. Antigament es podia compartir un recurs i posar-li un password d'accés al recurs, tothom que conaixia el pasword (que calia compartir) podia accedir al recurs.

Per els exercicis plantejats aquí amb equips ***stand alone*** la seguretat que cal usar és de tipus ***user*** i utilitzant com a base de dades d'usuaris/seguretat el mecanisme ***tdbsam***.

Aquest és un exemple de configuració de seguretat:

```
[global]
        workgroup = MYGROUP
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        security = user
        passdb backend = tdbsam
        load printers = yes
```

```
        cups options = raw
```

Repàs al model de treball

Aquest és un recordatori dels rols d'usuari que intervenen en una connexió samba per per exemple pujar un fitxer a un share.

Client unix
En un client unix som per exemple l'usuari *pere*. Aquest usuari és el que farà la connexió amb smbclient i els get i put. Allò que es descarregui amb get es desarà al seu home (per defecte) amb el seu usuari i grup i mode.

Usuari samba
L'usuari pere anterior realitza per exemple l'ordre: smbclient -U patipla //server/recurs. Està indicant que en el servidor samba es connectarà com a usuari *patipla*. Aquest ha de ser un usuari samba vàlid.
Els usuaris samba han de tenir un password samba assignat i es basen en usuaris unix existents en el sistema. **nota** Això és iaxí fent servir de backend *tdbsam*, però hi ha altres mecanismes com *ldapsam* amb característiques diferents.

Usuari unix destí
Quan l'usuari *pere* realitza accions en el sistema de fitxers (per exemple PUT, mkdir, rm, etc) ho fa en nom de l'usuari samba *patipla*, però les accions en el sistema de fitxers s'han de 'traduir', fer el **mapping**, a un usuari unix vàlid. Com és obvi samba fa el id mapping entre la usuaria samba *patipla* a la usuaria unix platipla.

Aquest últim pas el podem observar llistat la base de dades d'usuaris samba i observant que cada usuari té un ID que correspon al UID unix:

```
[root@samba docker]# pdbedit -L
patipla:1000:
roc:1002:
lila:1001:
pla:1003:
```

```
[root@samba docker]# tail -n4 /etc/passwd
patipla:x:1000:1000::/home/patipla:/bin/bash
lila:x:1001:1001::/home/lila:/bin/bash
roc:x:1002:1002::/home/roc:/bin/bash
pla:x:1003:1003::/home/pla:/bin/bash
```

La discoteca amb dos 'segurates'
Finalment recordar que sempre que estem parlant de serveis de xarxa es trobem amb el model que hem de creuar varis controls de seguretat. En l'accés remot al servei s'apliquen les regles del servei (permet samba l'accés al share? és el share readable/writable?, és un usuari amb drets?).
Un cop superats els permisos del servei si l'acció consisteix a actuar en el sistema de fitxers (desar, esborrar, llistar) llavors cal superar els permisos del sistema de fitxers. En aquest cas els permisos de unix del directori i dels fitxers. És a dir, per molt que samba ens deixi, si el directori no permet escriptura per a la usuaria *patipla* aquesta no podrà esborrar ni pujar-hi res.

Directori Home dels usuaris

Pot un usuari accedir al seu home via un recurs/share de samba? Evidentment que si. Primerament veurem una mala manera de fer-ho i després la manera com samba ja automatitza l'exportació dels homes dels usuaris

Una mala manera de treballar!

Amb aquest senzill exemple podem generar un share que exporta els homes dels usuaris en un recurs anomenat *myhome* (inventat). Observeu que la ruta del directori a exportar utilitza la variable %U que correspon al nom de l'usuari samba al que connectar.

```
[myhome]
        comment = Share amb els homes dels usuaris
        path = /home/%U
        writable = yes
        guest ok = no
        browseable = no
```

```
[root@hostedt tmp]# smbclient -U roc%roc //samba/myhome
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> ls
  .                   D        0  Fri Dec 14 16:44:38 2018
  ..                  D        0  Fri Dec 14 16:44:41 2018
  .bash_logout                H       18  Mon Jun 18 10:37:45 2018
  .bash_profile               H      193  Mon Jun 18 10:37:45 2018
  .bashrc                     H      231  Mon Jun 18 10:37:45 2018

                10474496 blocks of size 1024. 9892316 blocks available
smb: \> pwd
Current directory is \\samba\myhome\
smb: \> mkdir soc-en-roc
```

```
smb: \>
```

Observem de l'exemple anterior que *roc* s'ha connectat al recurs *myhome* i està realment al seu home (caldria haver-hi posat alguna dada privada seva per verificar-ho!). observem també que en una altra sessió la usuària *lila* quan accedeix al mateix recurs *myhome* en realitat no accedeix al de en *roc* sinó al seu home (al de la *lila*).

```
[root@hostedt ~]# smbclient -U lila%lila //samba/myhome
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> ls
  .                   D        0  Fri Dec 14 16:44:37 2018
  ..                  D        0  Fri Dec 14 16:44:41 2018
  .bash_logout                H       18  Mon Jun 18 10:37:45 2018
  .bash_profile               H      193  Mon Jun 18 10:37:45 2018
  .bashrc                     H      231  Mon Jun 18 10:37:45 2018

                10474496 blocks of size 1024. 9892332 blocks available
smb: \>
```

Exportar els home dels usuaris (una bona manera de treballar)

Samba automatitza l'exportació dels directoris home dels usuaris en un share que ve per defecte en la configuració (conjuntament amb el de impressores). Aquest recurs s'anomena ***[homes]***. Per defecte està activat, no és browseable i és de lectura/escriptura. S'hi poden aplicar restriccions d'accés limitant a quins usuaris se'ls permet connectar (del domini, servidor, provinents de uns determinats hosts, ips, networks, etc).

```
[homes]
        comment = Home Directories
        browseable = no
        writable = yes
;       valid users = %S
;       valid users = MYDOMAIN\%S
```

L'accés al home dels usuaris samba és molt senzill, via el share [homes], però ***NO*** usant aquest nom sinó indicant el nom de l'usuari. Així si la usuaria *patipla* vol accedir al seu home indicarà *//server/patipla*.

//server/nomusuari

```
[root@hostedt tmp]# smbclient -U roc%roc //samba/roc
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
```

```
smb: \> ls
  .                   D        0  Fri Dec 14 18:28:39 2018
  ..                  D        0  Fri Dec 14 16:44:41 2018
  .bash_logout                H       18  Mon Jun 18 10:37:45 2018
  .bash_profile               H      193  Mon Jun 18 10:37:45 2018
  .bashrc                     H      231  Mon Jun 18 10:37:45 2018
  soc-en-roc                  D        0  Fri Dec 14 18:28:39 2018

                10474496 blocks of size 1024. 9892316 blocks available
smb: \>
```

```
[root@hostedt ~]# smbclient -U patipla%patipla //samba/patipla
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.7.10]
smb: \> pwd
Current directory is \\samba\patipla\
smb: \> ls
  .                   D        0  Fri Dec 14 16:44:36 2018
  ..                  D        0  Fri Dec 14 16:44:41 2018
  .bash_logout                H       18  Mon Jun 18 10:37:45 2018
  .bash_profile               H      193  Mon Jun 18 10:37:45 2018
  .bashrc                     H      231  Mon Jun 18 10:37:45 2018

                10474496 blocks of size 1024. 9892352 blocks available
smb: \>
```

Global Options

General

```
[global]
        ...
[homes]
        ...
[printers]
        ...
[test]
        ...
```

Es poden definir opcions generals per defecte que poden ser redefinides per share:

```
[global]
        netbios name = toltec
        server string = Samba %v on %L
        workgroup = METRAN
        encrypt passwords = yes
        wins support = yes
        read only = no
```

En la configuració es poden usar variables com les definides en la taula 6-2 using samba:

```
%a    Client's architecture (see Table 6-1)
%I    Client's IP address (e.g., 172.16.1.2)
%m    Client's NetBIOS name
%M    Client's DNS name

%u    Current Unix username
%U    Requested client username (not always used by Samba)
%H    Home directory of %u
%g    Primary group of %u
%G    Primary group of %U

%S    Current share's name
%P    Current share's root directory
%p    Automounter's path to the share's root directory, if different from %P
%d    Current server process ID

%h    Samba server's DNS hostname
%L    Samba server's NetBIOS name
```

```
%N    Home directory server, from the automount map
%v    Samba version

%R    The SMB protocol level that was negotiated
%T    The current date and time
%$var    The value of environment variable var
```

Hosts Allow/Deny

1. If no allow or deny options are defined anywhere in smb.conf, Samba allows connections from any system.

2. If hosts allow or hosts deny options are defined in the [global] section of smb.conf, they determine general access to the server, even if either option is defined in one or more of the shares.

3. If only a hosts allow option is defined for a share, only the hosts listed are allowed to use the share. All others are denied.

4. If only a hosts deny option is defined for a share, any client that is not on the list can use the share.

5. If both a hosts allow option and a hosts deny option are defined, the allow list takes precendence. But if a host does not match the allow list or the deny list, it is granted implicit access.
Take care that you don't explicitly allow a host to access a share, but then deny access to the entire subnet of which the host is part.

Let's look at another example of that final item. Consider the following options:
hosts allow = 111.222.
hosts deny = 111.222.333.
In this case, hosts that belong to the subnet 111.222.*.* will be allowed access to the Samba shares.
The deny list in the case is completely disregarded because it is a subset of the allow list.

To allow all hosts in the 111.222.0.0/16 network except those on the 111.222.333.0/24 network, we can specify the following hosts allow shorthand notation:
hosts allow = 111.222. EXCEPT 111.222.333.

```
[global]
   #  Networking configuration options
   hosts allow = 192.168.220. 134.213.233.
   hosts deny = 192.168.220.102
```

```
interfaces = 192.168.220.100/255.255.255.0 \
             134.213.233.110/255.255.255.0
bind interfaces only = yes
```

1. If no allow or deny options are defined anywhere in *smb.conf*, Samba will allow connections from any system.
2. If hosts allow or hosts deny options are defined in the [global] section of *smb.conf*, they will apply to all shares, even if either option is defined in one or more of the shares.
3. If only a hosts allow option is defined for a share, only the hosts listed will be allowed to use the share. All others will be denied.
4. If only a hosts deny option is defined for a share, any client which is not on the list will be able to use the share.
5. If both a hosts allow option and a hosts deny option are defined, the allow list takes precendence. But if a host does not match the allow list or the deny list, it is granted implicit access.

hosts allow

You can specify any of the following formats for this option:

- Hostnames, such as ftp.example.com .
- IP addresses, such as 130.63.9.252.
- Domain names, which can be differentiated from individual hostnames because they start with a dot. For example, .ora.com represents all systems within the *ora.com* domain.
- Netgroups, which start with an at sign (@), such as @printerhosts. Netgroups are usually available only on systems running NIS or NIS+. If netgroups are supported on your system, there should be a netgroups manual page that describes them in more detail.
- Subnets, which end with a dot. For example, 130.63.9. means all the systems whose IP addresses begin with 130.63.9.
- The keyword ALL, which allows any client access.
- The keyword EXCEPT followed by one or more names, IP addresses, domain names, netgroups, or subnets. For example, you could specify that Samba allow all hosts except those on the 192.168.110 subnet with hosts allow = ALL EXCEPT 192.168.110. (remember to include the trailing dot).

TIP

If you specify hosts allow in the [global] section, that definition will override any hosts allow lines in the share definitions. This is the opposite of the usual behavior, which is for parameters set in share definitions to override default values set in the [global] section.

Logging

```
[global]
```

```
log level = 2
log file = /var/log/samba.log.%m
max log size = 50
debug timestamp = yes
```

```
[root@c2ae73d0f616 /]# ll /var/log/samba/
drwx------ 4 root root 4096 Nov 11 21:59 cores
-rw-r--r-- 1 root root  148 Nov 11 22:38 log.
-rw-r--r-- 1 root root 2481 Dec  1 07:24 log.nmbd
-rw-r--r-- 1 root root 8506 Dec  1 07:25 log.smbd
drwx------ 2 root root 4096 Aug 31 16:22 old
```

Name Resolution & Browsing

Documentation: Samba documentation Chapter 7 Name Resolution and Browsing

Name Resolution

Per ajudar una mica a l'impresentable organització de xarxa via browsing es va desenvolupar WINS, un protocol de noms per a Windows (correcte, encara no s'han enterat del DNS!).

Un server windows pot actuar com a servidor de noms de Netbeui si es configura com a servidor WINS. Els altres hosts li demanen que resolgui els noms Netbeui a adreces IP.

```
name resolve order = ...
wins server = yes/adreçaIP
wins support = yes/no
```

wins server: amb aquests opció a *yes* s'indica que el servidor realitza la funció de servidor de noms WINS. Si ha d'actuar com a client WINS llavors en lloc de yes cal configurar l'*adreça IP* del servidor WINS.

wins support: activada a yes fa que els hosts de la xarxa actuïn com a clients de WINS.

Imitant el funcionament del fitxer /etc/hosts dels sistemes GNU/Linux en entorns Windows s'utilitza per a la resolució local de noms Netbeui el fitxer ***/etc/samba/lmhosts*** (originari de Lan Manager).

Resolució Windows host clients

Utilització de lmhosts

```
[root@hp01 ~]# cat /etc/samba/lmhosts
127.0.0.1 localhost
172.17.0.5 2EA1AC403693
172.17.0.8 3C7C3716C3AB
172.17.0.2 3145DBF85061
172.17.0.4 939C09590BDC

[root@hp01 ~]# nmblookup 939C09590BDC
172.17.0.4 939C09590BDC<00>
```

```
[root@3145dbf85061 /]# nmblookup -S 939C09590BDC
172.17.0.4 939C09590BDC<00>
Looking up status of 172.17.0.4
   939C09590BDC    <00> -          B <ACTIVE>
   939C09590BDC    <03> -          B <ACTIVE>
   939C09590BDC    <20> -          B <ACTIVE>
   MYGROUP         <00> - <GROUP> B <ACTIVE>
   MYGROUP         <1e> - <GROUP> B <ACTIVE>

   MAC Address = 00-00-00-00-00-00
```

[root@939c09590bdc /]# nmblookup -S 3145DBF85061 *(és el Master Browser)*

```
172.17.0.8 3145DBF85061<00>
Looking up status of 172.17.0.8
   3145DBF85061    <00> -          B <ACTIVE>
   3145DBF85061    <03> -          B <ACTIVE>
   3145DBF85061    <20> -          B <ACTIVE>
   ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>
   MYGROUP         <00> - <GROUP> B <ACTIVE>
   MYGROUP         <1d> -          B <ACTIVE>
   MYGROUP         <1e> - <GROUP> B <ACTIVE>

   MAC Address = 00-00-00-00-00-00
```

Utilització de Wins

```
# This section details the support for the Windows Internet Name Service (WINS).
# Note: Samba can be either a WINS server or a WINS client, but not both.

# wins support = when set to yes, the NMBD component of Samba enables its WINS
# server.
#
# wins server = tells the NMBD component of Samba to be a WINS client.

# wins proxy = when set to yes, Samba answers name resolution queries on behalf
# of a non WINS capable client. For this to work, there must be at least one
# WINS server on the network. The default is no.

# dns proxy = when set to yes, Samba attempts to resolve NetBIOS names via DNS
# nslookups.
```

Resolució GNU/Linux hosts clients

```
[root@hp01 ~]# vim /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1              localhost6.localdomain6 localhost6
172.17.0.3      2EA1AC403693
172.17.0.5      3C7C3716C3AB
```

El servei nmbd

La resolució de noms windows la realitza el servei */usr/sbin/nmbd*. Podeu observar que si atureu el servei la resolució de noms windows, per exemple amb nmblookup, deixa de funcionar.

Master Browser

Una mica d'història: les xarxes windows s'originen sense implementar un servei DNS i els equips s'identifiquen per un nom de 15 caràcters usat pel protocol NETBEUI. Per saber quins equips hi ha a la xarxa local Windows implementa un mètode espectacular, fer crits! via *broadcasts* els equips s'identifiquen els uns amb els altres. Aquesta tecnologia punta evoluciona i apareix la funció d'encarregat principal de la xarxa, que anota els noms de tots els equips que van apareixent a la xarxa i els va difonent a qui els hi demana.

Tot aquest refregit provoca allò tan tradicional en Windows de clicar a la icona de la xarxa i creuar els dits a veure quins equips apareixen i quins no. Evidentment la informació que es mostra no és mai fidedigna, es una foto dels equips que han contestat en algun moment o altre, però en poden faltar i pot ser que d'altres ja no hi siguin.

En una xarxa Windows entre hosts on no hi ha un PDC (Controlador de domini) els equips competeixen entre ells per escollir un *local master browser*. Aquest procés s'anomena **Eleccions**.

El procés d'eleccions es dirimeix en:

- Valor del sistema operatiu: *os-value*.
- Valor del *computer role*.
- Temps que el sistema està up.
- Menor nom Netbeui del host.
- Si a la CUP no li cau bé no pot ser-ho!

Tota subxarxa local escull el seu local *master browser*. Si aquestes diverses xarxes estan sota un Domini Windows (un PDC) llavors s'escull també un *Domain Master Browser*.

```
local master = no/yes
os level = nº
preferred master = no/yes
```

Directives per a fer de *Local Master Browser*:

- **local master**: el valor *no* indica que l'equip refusa ser mai *local master browser*. El valor *yes* vol dir que es postula per ser-ho, però no que ho sigui, li caldrà guanyar la *election*.
- **os level**: indica un valor que com major és més dret a ser el *master browser* té. Aquest valor depèn de la versió del sistema operatiu però es pot establir arbitràriament.
- **preferred master**: el valor yes indica que l'equip vol ser *master browser* i força (quan s'inicia) que es produeixi una nova *election*. És a dir, força eleccions.

Primer Cas

Donats dos hosts amb SAMBA server que no juguen cap rol de PDC podem observar que un d'ells realitza la funció de *Local Master Browser*.

```
[root@3c7c3716c3ab /]# smbtree
Enter GUEST's password:
MYGROUP
    \\3C7C3716C3AB              Samba Server Version 4.2.3
        \\3C7C3716C3AB\IPC$             IPC Service (Samba Server Version 4.2.3)
        \\3C7C3716C3AB\public           Share de contingut public
        \\3C7C3716C3AB\manpages         Documentació man del container
        \\3C7C3716C3AB\documentation    Documentació doc del container
    \\2EA1AC403693              Samba Server Version 4.2.3
        \\2EA1AC403693\IPC$             IPC Service (Samba Server Version 4.2.3)
        \\2EA1AC403693\public           Share de contingut public
        \\2EA1AC403693\manpages         Documentació man del container
        \\2EA1AC403693\documentation    Documentació doc del container

[root@3c7c3716c3ab /]# smbtree -D
Enter GUEST's password:
MYGROUP
[root@3c7c3716c3ab /]# smbtree -S
Enter GUEST's password:
MYGROUP
    \\3C7C3716C3AB    Samba Server Version 4.2.3
    \\2EA1AC403693              Samba Server Version 4.2.3
```

```
[root@3c7c3716c3ab /]# smbclient  -L 3C7C3716C3AB
Enter GUEST's password:
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Sharename           Type    Comment
    ---------       ----    -------
    documentation   Disk        Documentació doc del container
    manpages        Disk        Documentació man del container
    public           Disk       Share de contingut public
    IPC$             IPC        IPC Service (Samba Server Version 4.2.3)
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Server               Comment
    ---------       -------
    3C7C3716C3AB    Samba Server Version 4.2.3
    Workgroup            Master
    ---------       -------
    MYGROUP

[root@3c7c3716c3ab /]# smbclient  -L 2EA1AC403693
Enter GUEST's password:
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Sharename           Type    Comment
    ---------       ----    -------
    documentation   Disk        Documentació doc del container
    manpages        Disk        Documentació man del container
    public           Disk       Share de contingut public
    IPC$             IPC        IPC Service (Samba Server Version 4.2.3)
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Server               Comment
    ---------       -------
    2EA1AC403693    Samba Server Version 4.2.3
    3C7C3716C3AB    Samba Server Version 4.2.3
    Workgroup            Master
    ---------       -------
    MYGROUP          2EA1AC403693
```

Segon Cas

Generem dos containers Docker més de SAMBA ambdós del WorkGroup NEWGROUP i a un d'ells li modifiquem les opcions per forçar que sigui *master browser*:

```
[global]
        workgroup = NEWGROUP
        server string = Samba Server Version %v 2HISIX
        local master = yes
        os level = 33
        preferred master = yes
```

```
# ----------------------- Browser Control Options ----------------------------
# local master = when set to no, Samba does not become the master browser on
# your network. When set to yes, normal election rules apply.

# os level = determines the precedence the server has in master browser
# elections. The default value should be reasonable.

# preferred master = when set to yes, Samba forces a local browser election at
# start up (and gives itself a slightly higher chance of winning the election).
```

```
[root@939c09590bdc /]# smbtree -D
Enter GUEST's password:
NEWGROUP
MYGROUP

[root@939c09590bdc /]# smbtree -S
Enter GUEST's password:
NEWGROUP
    \\939C09590BDC              Samba Server Version 4.2.3 2HISIX
    \\3145DBF85061              Samba Server Version 4.2.3 2HISIX
MYGROUP
    \\3C7C3716C3AB    Samba Server Version 4.2.3
    \\2EA1AC403693              Samba Server Version 4.2.3
```

```
root@939c09590bdc /]# smbclient -L 3145DBF85061
Enter GUEST's password:
Anonymous login successful
Domain=[NEWGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Sharename       Type      Comment
    ---------       ----      -------
    documentation   Disk      Documentació doc del container
    manpages        Disk      Documentació man del container
    public          Disk      Share de contingut public
    IPC$            IPC       IPC Service (Samba Server Version 4.2.3 2HISIX)
Anonymous login successful
Domain=[NEWGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Server               Comment
    ---------       -------
```

```
    3145DBF85061    Samba Server Version 4.2.3 2HISIX
    939C09590BDC    Samba Server Version 4.2.3 2HISIX
    Workgroup       Master
    ---------       -------
    MYGROUP         2EA1AC403693
    NEWGROUP        939C09590BDC
```

Tercer Cas

Donats quatre containers Docker configurats com a Samba Server (no PDC) modificar en un d'ells el valor de *os level* i *preferred master* per fer-lo *master browser*.

```
[root@3145dbf85061 /]# smbtree -S
Enter GUEST's password:
MYGROUP
    \\3C7C3716C3AB    Samba Server Version 4.2.3
    \\3145DBF85061          Samba Server Version 4.2.3 2HISIX
    \\2EA1AC403693          Samba Server Version 4.2.3

[root@3145dbf85061 /]# smbclient -L 2EA1AC403693
Enter GUEST's password:
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Sharename       Type    Comment
    documentation   Disk    Documentació doc del container
    manpages        Disk    Documentació man del container
    public          Disk    Share de contingut public
    IPC$            IPC     IPC Service (Samba Server Version 4.2.3)
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Server          Comment
    2EA1AC403693    Samba Server Version 4.2.3
    3145DBF85061    Samba Server Version 4.2.3 2HISIX
    3C7C3716C3AB    Samba Server Version 4.2.3
    Workgroup       Master
    MYGROUP         2EA1AC403693
```

```
        local master = yes
        os level = 50
        preferred master = yes
```

```
[root@939c09590bdc /]# smbtree -S
```

```
Enter GUEST's password:
MYGROUP
    \\939C09590BDC          Samba Server Version 4.2.3 2HISIX
    \\3C7C3716C3AB    Samba Server Version 4.2.3
    \\3145DBF85061          Samba Server Version 4.2.3 2HISIX
    \\2EA1AC403693          Samba Server Version 4.2.3

[root@939c09590bdc /]# smbclient  -L 939C09590BDC
Enter GUEST's password:
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Sharename       Type    Comment
    documentation   Disk    Documentació doc del container
    manpages        Disk    Documentació man del container
    public          Disk    Share de contingut public
    IPC$            IPC     IPC Service (Samba Server Version 4.2.3 2HISIX)
Anonymous login successful
Domain=[MYGROUP] OS=[Windows 6.1] Server=[Samba 4.2.3]
    Server              Comment
    2EA1AC403693    Samba Server Version 4.2.3
    3145DBF85061    Samba Server Version 4.2.3 2HISIX
    3C7C3716C3AB    Samba Server Version 4.2.3
    939C09590BDC    Samba Server Version 4.2.3 2HISIX
    Workgroup           Master
    MYGROUP             939C09590BDC
```

[root@939c09590bdc /]# nmblookup -S 3145DBF85061 *(és el Master Browser)*

```
172.17.0.8 3145DBF85061<00>
Looking up status of 172.17.0.8
    3145DBF85061    <00> -          B <ACTIVE>
    3145DBF85061    <03> -          B <ACTIVE>
    3145DBF85061    <20> -          B <ACTIVE>
    ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>
    MYGROUP         <00> - <GROUP> B <ACTIVE>
    MYGROUP         <1d> -          B <ACTIVE>
    MYGROUP         <1e> - <GROUP> B <ACTIVE>

    MAC Address = 00-00-00-00-00-00
```

```
[2015/11/17 22:26:43.291355,  0] ../lib/util/become_daemon.c:124(daemon_ready)
  STATUS=daemon 'nmbd' finished starting up and ready to serve connections
[2015/11/17 22:27:06.070962,  0]
../source3/nmbd/nmbd_become_lmb.c:397(become_local_master_stage2)
  *****
```

Samba name server 939C09590BDC is now a local master browser for workgroup

```
MYGROUP on subnet 172.17.0.10
  *****
```

Domain Master Browser

Existeixen dos tipus de browsing:

- Local Master Browsing.
- Domain Master Browsing.

Local Master Browsing: explicat en l'apartat anterior. Cada subxarxa escull via *election* qui fa aquesta funció.

Domain Master Browsing: donades múltiples subxarxes diferents en un Domini Windows, gestionat per un PDC Controlador Principal de Domini, aquest equip realitza la funció de Domain Master Browsing i Local Master Browsing. les dues funcions.
No s'escull per elecció sinó que l'administrador ho configura amb les opcions:

```
domain master = yes/no
preferred master = yes/no
local master = yes/no
os level = nº
```

Rols del servidor SAMBA

Rols

El servidor SAMBA pot realitzar els rols següents:

- Servidor Standalone.
- PDC Controlador Principal de domini.
- Member Server.
- Browser.
- Name resolution.

```
# ----------------------- Standalone Server Options ----------------------
# security = the mode Samba runs in. This can be set to user, share (deprecated), or server
(deprecated).
# passdb backend = the backend used to store user information in. New installations should
use either tdbsam or ldapsam. No additional configuration is required for tdbsam. The
"smbpasswd" utility is available for backwards compatibility.
        security = user
        passdb backend = tdbsam
```

```
# ----------------------- Domain Controller Options ----------------------
# security = must be set to user for domain controllers.
# passdb backend = the backend used to store user information in. New installations should
use either tdbsam or ldapsam. No additional configuration is required for tdbsam. The
"smbpasswd" utility is available for backwards compatibility.
# domain master = specifies Samba to be the Domain Master Browser, allowing Samba to
collate browse lists between subnets. Do not use the "domain master" option if you already
have a Windows NT domain controller performing this task.
# domain logons = allows Samba to provide a network logon service for Windows
workstations.
# logon script = specifies a script to run at login time on the client. These scripts must be
provided in a share named NETLOGON.
# logon path = specifies (with a UNC path) where user profiles are stored.
;       security = user
;       passdb backend = tdbsam
;       domain master = yes
;       domain logons = yes
        # the following login script name is determined by the machine name
        # (%m):
;       logon script = %m.bat
        # the following login script name is determined by the UNIX user used:
;       logon script = %u.bat
```

```
;	logon path = \\%L\Profiles\%u
	# use an empty path to disable profile support:
;	logon path =
	# various scripts can be used on a domain controller or a stand-alone
	# machine to add or delete corresponding UNIX accounts:
;	add user script = /usr/sbin/useradd "%u" -n -g users
;	add group script = /usr/sbin/groupadd "%g"
;	add machine script = /usr/sbin/useradd -n -c "Workstation (%u)" -M -d /nohome -s
/bin/false "%u"
;	delete user script = /usr/sbin/userdel "%u"
;	delete user from group script = /usr/sbin/userdel "%u" "%g"
;	delete group script = /usr/sbin/groupdel "%g"
```

```
# ----------------------- Domain Members Options -----------------------
# security = must be set to domain or ads.
# passdb backend = the backend used to store user information in. New installations should
use either tdbsam or ldapsam. No additional configuration is required for tdbsam. The
"smbpasswd" utility is available for backwards compatibility.
# realm = only use the realm option when the "security = ads" option is set. The realm option
specifies the Active Directory realm the host is a part of.
# password server = only use this option when the "security = server" option is set, or if you
cannot use DNS to locate a Domain Controller. The argument list can include
My_PDC_Name, [My_BDC_Name], and [My_Next_BDC_Name]:
# password server = My_PDC_Name [My_BDC_Name] [My_Next_BDC_Name].
# Use "password server = *" to automatically locate Domain Controllers.
;	security = domain
;	passdb backend = tdbsam
;	realm = MY_REALM
;	password server = <NT-Server-Name>
```

```
# ----------------------- Browser Control Options ----------------------------
# local master = when set to no, Samba does not become the master browser on your
network. When set to yes, normal election rules apply.
# os level = determines the precedence the server has in master browser elections. The
default value should be reasonable.
# preferred master = when set to yes, Samba forces a local browser election at start up (and
gives itself a slightly higher chance of winning the election).
;	local master = no
;	os level = 33
;	preferred master = yes
```

```
#---------------------------- Name Resolution ------------------------------
# This section details the support for the Windows Internet Name Service (WINS).
# Note: Samba can be either a WINS server or a WINS client, but not both.
```

```
# wins support = when set to yes, the NMBD component of Samba enables its WINS
# server.
# wins server = tells the NMBD component of Samba to be a WINS client.
# wins proxy = when set to yes, Samba answers name resolution queries on behalf of a non
WINS capable client. For this to work, there must be at least one  WINS server on the
network. The default is no.
# dns proxy = when set to yes, Samba attempts to resolve NetBIOS names via DNS
# nslookups.
;       wins support = yes
;       wins server = w.x.y.z
;       wins proxy = yes
;       dns proxy = yes
```

Role Standalone

```
[root@portatil samba]# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[public]"
Processing section "[documentacio]"
Processing section "[repositori]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
```

```
[global]
    workgroup = GRUPM06
    netbios name = SMBSERVER
    server string = edt - Samba Server Version %v
    log file = /var/log/samba/log.%m
    max log size = 50
    wins support = Yes
    idmap config * : backend = tdb
    cups options = raw

[homes]
    comment = Home Directories
    read only = No
    browseable = No

[printers]
    comment = All Printers
    path = /var/spool/samba
```

```
    printable = Yes
    print ok = Yes
    browseable = No

[public]
    comment = Public Stuff
    path = /var/lib/samba/shares/public
    read only = No
    guest ok = Yes

[documentacio]
    comment = System Documentation
    path = /var/lib/samba/shares/samba-docs
    guest ok = Yes

[repositori]
    comment = Repositori de dades
    path = /var/lib/samba/shares/repositori
    write list = +staff
    read only = No
    guest ok = Yes
```

```
[root@portatil samba]# smbclient -U% -L localhost

Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
    Sharename       Type      Comment
    ---------       ----      -------
    IPC$            IPC       IPC Service (edt - Samba Server Version 3.6.12-1.fc17)
    repositori      Disk      Repositori de dades
    documentacio    Disk      System Documentation
    public          Disk      Public Stuff
    Cups-PDF        Printer   Cups-PDF
    ClassPDF        Printer   Classe PF printers

Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
    Server               Comment
    ---------            -------
    SMBSERVER            edt - Samba Server Version 3.6.12-1.fc17

    Workgroup            Master
    ---------            -------
    GRUPM06              SMBSERVER
```

```
[pere@portatil ~]$ smbtree
Enter pere's password:
GRUPM06
```

```
\\SMBSERVER                    edt - Samba Server Version 3.6.12-1.fc17
        \\SMBSERVER\ClassPDF           Classe PF printers
        \\SMBSERVER\Cups-PDF           Cups-PDF
        \\SMBSERVER\public             Public Stuff
        \\SMBSERVER\documentacio       System Documentation
        \\SMBSERVER\repositori         Repositori de dades
        \\SMBSERVER\IPC$               IPC Service (edt - Samba Server …..fc17)
```

Rol PDC Domain Server

```
[root@c2ae73d0f616 /]# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[documentation]"
Processing section "[manpages]"
Processing section "[public]"
Processing section "[privat]"
Loaded services file OK.
WARNING: You have some share names that are longer than 12 characters.
These may not be accessible to some older clients.
(Eg. Windows9x, WindowsMe, and smbclient prior to Samba 3.0.)
Server role: ROLE_DOMAIN_PDC
```

Repàs ordres client

Smbclient

```
]$ smbclient  -L smbserver
Enter unknowns's password:
Anonymous login successful

Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
   Sharename          Type    Comment
   ---------          ----    -------
   public         Disk    Public Stuff
   documentacio           Disk    System Documentation
   repositori     Disk    Repositori de dades
   IPC$           IPC     IPC Service (edt - Samba Server Version 3.6.12-1.fc17)
   Cups-PDF               Printer   Cups-PDF
   ClassPDF               Printer   Classe PF printers
Anonymous login successful

Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
   Server               Comment
   SMBSERVER            edt - Samba Server Version 3.6.12-1.fc17

   Workgroup            Master
   GRUPM06              SMBSERVER
```

Usuaris autenticats:

```
[pere@client ~]$ smbclient //smbserver/public
Enter pere's password:
session setup failed: NT_STATUS_LOGON_FAILURE
```

```
[root@smbserver samba]# smbpasswd -a pere
New SMB password:
Retype new SMB password:
Added user pere.
```

```
[pere@clientl ~]$ smbclient //smbserver/public
Enter pere's password:
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
smb: \>
```

```
[pau@client ~]$ smbclient //smbserver/public
Enter pau's password:
session setup failed: NT_STATUS_LOGON_FAILURE
```

```
[pau@client ~]$ smbclient //smbserver/public -U guest
Enter guest's password:
Anonymous login successful
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
smb: \>
```

```
[pere@client ~]$ smbclient //smbserver/documentacio
Enter pere's password:
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
smb: \> quit

[pere@client ~]$ smbclient //smbserver/documentacio pere
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
smb: \> quit

[pere@client ~]$ smbclient //smbserver/documentacio -U pere%pere
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
smb: \> quit
```

```
smb: \> help
ls              dir             du              lcd             cd
pwd             get             mget            put             mput
rename          more            mask            del             open
rm              mkdir           md              rmdir           rd
prompt          recurse         translate       lowercase       print
printmode       queue           cancel          quit            q
exit            newer           archive         tar             blocksize
tarmode         setmode         help            ?               history
!
```

```
unix2dos
dos2unix
```

Ordres desateses:

```
$ smbclient //smbserver/public -c "ls " -U pere%pere |   grep "^  " | cut -d ' ' -f 3 - | sort
```

```
$ alias smbls='smbclient //smbserver/public -c \"ls \" -U pere%pere |   grep "^  " | cut -d\  -f 3 -
```

```
| sort

$ smbls
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
.
..
A05-14-serveisxarxa.pdf
activitats_asix_m06_uf1_nf5_2014-2015.pdf
```

```
smbls(  )
{
        share=`echo $1 | cut -d '/' -f '1-4'`
        dir=`echo $1 | cut -d '/' -f '5-'`
        smbclient $share -c "cd $dir; ls" -A ~/.smbpw | \
                grep "^  " | cut -d ' ' -f 3 - | sort
}
```

Shares Backups

```
[pere@client ~]$ smbclient //smbserver/public -U pere%pere -Tc public.tar
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
          159579 ( 3315,7 kb/s) \A05-14-serveisxarxa.pdf
          66227 (64674,8 kb/s) \activitats_asix_m06_uf1_nf5_2014-2015.pdf
tar: dumped 2 files and directories
Total bytes written: 226304

[pere@client ~]$ ll public.tar
-rw-r--r-- 1 pere pere 228352 15 nov 19:11 public.tar

[pere@client ~]$ tar tvf public.tar
-rw-r--r-- 0/0             159579 2014-11-15 17:21 ./A05-14-serveisxarxa.pdf
-rw-r--r-- 0/0             66227 2014-11-15 17:15 ./activitats_asix_m06_uf1_nf5_2014-2015.pdf
```

```
[pere@client ~]$ smbclient //smbserver/public -U pere%pere
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.6.12-1.fc17]
smb: \> tarmode full hidden system quiet
tarmode is now full, system, hidden, noreset, quiet
smb: \> tar c public2.tar
tar: dumped 2 files and directories
Total bytes written: 226304
smb: \> quit

[pere@client ~]$ ll public2.tar
-rw-r--r-- 1 pere pere 228352 15 nov 19:17 public2.tar
```

cifs - smbfs

```
[root@client ~]# yum install cifs-utils
```

```
[root@client ~]# mount -t cifs //127.0.01/public /mnt -o user=pere,password=pere

[root@client ~]# mount | grep cifs
//127.0.01/public on /mnt type cifs
(rw,nosuid,nodev,noexec,relatime,vers=1.0,sec=ntlmssp,cache=strict,unc=\\127.0.01\public,
username=pere,domain=SMBSERVER,uid=0,noforceuid,gid=0,noforcegid,addr=127.0.0.1,u
nix,posixpaths,serverino,acl,rsize=1048576,wsize=65536,actimeo=1)

[root@client ~]# ls /mnt/
A05-14-serveisxarxa.pdf  activitats_asix_m06_uf1_nf5_2014-2015.pdf

[root@client ~]# umount /mnt
```

```
# mount -t cifs //127.0.01/public /mnt -o guest
# mount -t cifs //127.0.01/public /mnt -o user=pere,password=pere
# mount -t cifs //127.0.01/public /mnt -o credentials=file_passwd.txt
# mount -t cifs //127.0.01/public /mnt -o user=pere,password=pere,\
                                         uid=pere,gid=pere,file_mode=0664,dir_mode=0775
```

```
[root@client ~]# mount -t cifs //127.0.01/public /mnt -o
guest,uid=pere,gid=pere,file_mode=0644,dir_mode=0755

[root@client ~]# uname -a > /mnt/uname.txt
[root@client ~]# ls -la  /mnt/
drwxrwxrwx   2 pere pere      0 15 nov 19:56 .
drwxr-xr-x.   24 root root   4096 15 nov 14:04 ..
-rw-rw-r-- 1 pere pere 159579 15 nov 17:21 A05-14-serveisxarxa.pdf
-rw-rw-r-- 1 pere pere  66227 15 nov 17:15 activitats_asix_m06_uf1_nf5_2014-2015.pdf
-rw-r--r-- 1 pere pere 113 15 nov 19:53 uname.txt

[root@client ~]# mkdir /mnt/noudir
[root@portatil samba]# ls -ld /mnt/noudir/
drwxr-xr-x 2 pere pere 0 15 nov 19:59 /mnt/noudir/
```

Múltiples Samba Servers

```
[pere@client ~]$ smbtree
Enter pere's password:
GRUPM06
    \\SMBSERVER                     edt - Samba Server Version 3.6.12-1.fc17
        \\SMBSERVER\ClassPDF            Classe PF printers
        \\SMBSERVER\NullPrinter-01    Printer /dev/null
        \\SMBSERVER\ClassNulls          Classe de NullPrinters
        \\SMBSERVER\ClassAll            Classe amb totes les impressores
        \\SMBSERVER\NullPrinter-02    Priner /dev/null
        \\SMBSERVER\Virtual_PDF_Printer   Virtual PDF Printer
        \\SMBSERVER\Cups-PDF            Cups-PDF
        \\SMBSERVER\public              Public Stuff
        \\SMBSERVER\documentacio        System Documentation
        \\SMBSERVER\repositori          Repositori de dades
        \\SMBSERVER\IPC$                IPC Service (edt - Samba Version 3.6.12-1.fc17)
    \\SMBHP1                        edt - Samba Server Version 3.4.9-60.fc12
        \\SMBHP1\IPC$               IPC Service (edt - Samba Server Version 3.4.9-60.fc12)
        \\SMBHP1\hprepositori       Repositori de dades
        \\SMBHP1\hpdocumentacio     System Documentation
        \\SMBHP1\hppublic           Public Stuff
```

```
[pere@client ~]$ smbclient -L smbhp1
Enter pere's password:
Anonymous login successful
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.4.9-60.fc12]
    Sharename       Type    Comment
    hppublic        Disk    Public Stuff
    hpdocumentacio  Disk    System Documentation
    hprepositori    Disk    Repositori de dades
    IPC$            IPC     IPC Service (edt - Samba Server Version 3.4.9-60.fc12)
Anonymous login successful
Domain=[GRUPM06] OS=[Unix] Server=[Samba 3.4.9-60.fc12]
    Server          Comment
    SMBHP1          edt - Samba Server Version 3.4.9-60.fc12
    SMBSERVER       edt - Samba Server Version 3.6.12-1.fc17
    Workgroup       Master
    GRUPM06         SMBSERVER
```

```
# ------------------------------------------------------------------------------------
#  Example M06-ASO configuration: samba workgroup => master browser
# ------------------------------------------------------------------------------------
        workgroup = GRUPM06
        server string = edt - Samba Server Version %v
        netbios name = smbserver
        encrypt passwords = yes
        wins support = yes
```

```
        read only = no
        local master = yes
        os level = 34
        preferred master = yes
```

```
# ------------------------------------------------------------------------------------------------
#  Example M06-ASO configuration: samba workgroup  => member, no master
# ------------------------------------------------------------------------------------------------
        workgroup = GRUPM06
        server string = edt - Samba Server Version %v
        netbios name = smbhp1
        encrypt passwords = yes
        wins support = no
        read only = no
        # local master = no
        # os level = 33
        # preferred master = no
```

Altres:

samba & ldap
Samba & Ldap the official ubuntu documentation

passwd backend de tdsam: observar les ordres de unix que permeten crear usuaris, grups, màquines, etc

Pràctiques

Pràctica 1: Homes Samba

Muntar dins dels homes dels usuaris un altre home (com a classe) via samba.
Cal instal·lar els paquets samba i *cifs-utils-6.7-1.fc24.x86_64*
Configurar pam_mount.conf.xml: *<volume user="*" fstype="cifs" server="samba" path="%(USER)" mountpoint="~/%(USER)" />*

```
[root@host docker]# su - local01
[local01@host ~]$ su - anna
pam_mount password:

[anna@host ~]$ ll
total 0
drwx------+ 2 anna alumnes 0 Dec 14 18:31 anna

[anna@host ~]$ mount -t cifs
//samba/anna on /tmp/home/anna/anna type cifs
(rw,relatime,vers=1.0,cache=strict,username=anna,domain=,uid=5002,forceuid,gid=600,force
gid,addr=172.21.0.2,unix,posixpaths,serverino,mapposix,acl,rsize=1048576,wsize=65536,ech
o_interval=60,actimeo=1)
```

Pràctica 2: LDAP + Samba + PAM

Usant el servidor LDAP amb els usuaris habituals, un servidor SAMBA que reconeix els usuaris de LDAP i un host PAM que permet autenticació local i LDAP. Als usuaris locals es munta un directori tmp de tmpfs de 100M. Als usuaris LDAP es munta el seu home dins del home via samba.

Practica: SAMBA + LDAP + PAM

Podeu trobar la documentació GitHub d'aquesta practica a edtasixm06
Podeu trobar les imatges docker al Dockehub de edtasixm06
Podeu trobar la documentació del mòdul a ASIX-M06
ASIX M06-ASO Escola del treball de barcelona

Imatges:

- **edtasixm06/samba:18ldapusers** Servidor SAMBA amb usuaris locals i usuaris LDAP (unix). Es creen comptes d'usuari samba de usuaris locals i de alguns dels usuaris ldap (no tots). Es creen també els directoris home dels usuaris de ldap i se'ls assigna la pripietat/grup pertinent. Finalment s'exporten els *shares* d'exemple usuals i els **[homes]** dels usuaris samba. D'aquesta manera un hostpam (amb ldap) pot muntar els homes dels usuaris (home dins home) usant samba.

- **edtasixm06/ldapserver:18group** incorpora els posixGroup dels usuaris (per memberUid).

- **edtasixm06/hostpam:18mount** host pam amb authenticació ldap. utilitza l'ordre authconfig per configurar l'autenticació i a més a més crea els home dels usuaris i munta un tmpfs als usuaris. Atenció, per poder realitzar el mount cal que el container es generi amb l'opció **--privileged**.
  Poser en lloc d'aquest preferim usar el **edtasixm06/hostpam:18homenfs**

Arquitectura

Per implementar un host amb usuaris unix i ldap on els homes dels usuaris es muntin via samba de un servidor de disc extern cal:

- **sambanet** Una xarxa propia per als containers implicats.

- **ldapserver** Un servidor ldap en funcionament amb els usuaris de xarxa.

- **samba** Un servidor samba que exporta els homes dels usuaris com a shares via *[homes]* Caldrà fer les tasques següents en el servidor samba:

    - *Usuaris unix* Samba requereix la existència de usuaris unix. Per tant caldrà disposar dels usuaris unix, poden ser locals o de xarxa via LDAP. Així doncs, el servidor samba ha d'estar configurat amb nscd i nslcd per poder accedir al ldap. Amb getent s'han de poder llistar tots els usuaris i grups de xarxa.

- *homes* Cal que els usuaris tinguin un directori home. Els usuaris unix local ja en tenen en crear-se l'usuari, però els usuaris LDAP no. Per tant cal crear el directori home dels usuaris ldap i assignar-li la propietat i el grup de l'usuari apropiat.

- *Usuaris samba* Cal crear els comptes d'usuari samba (recolsats en l'existència del mateix usuari unix). Per a cada usuari samba els pot crear amb *smbpasswd* el compte d'usuasi samba assignant-li el password de samba. Convé que sigui el mateix que el de ldap per tal de que en fer login amb un sol password es validi l'usuari (auth de pam_ldap.so) i es munti el home via samba (pam_mount.so). Samba pot desar els seus usuaris en una base de dades local anomenada **tdbsam** o els pot desar en un servidor ldap usant com a backend **ldapsam**. El mecanisme més simple és usar *tdbsam* i *smbpasswd* i *pdbedit* com a utilitats.

- **hostpam** Un hostpam configurat per accedir als usuaris locals i ldap i que usant pam_mount.so munta dins del home dels usuaris un home de xarxa via samba. Cal configurar */etc/security/pam_mount.conf.xml* per muntar el recurs samba dels *[homes]* (i incloure el paquet cifs-utils).z

Execució

```
docker network create sambanet
docker run --rm --name ldap -h ldap --net sambanet -d edtasixm06/ldapserver:18group

docker run --rm --name samba -h samba --net sambanet -it edtasixm06/samba:18ldapusers

docker run --rm --name host -h host --net sambanet -it edtasixm06/hostpam:18homenfs
#canviar per :18homesamba
```

Configuració samba clau

```
[global]
	workgroup = MYGROUP
	server string = Samba Server Version %v
	log file = /var/log/samba/log.%m
	max log size = 50
	security = user
	passdb backend = tdbsam
	load printers = yes
```

```
        cups options = raw
[homes]
        comment = Home Directories
        browseable = no
        writable = yes
;       valid users = %S
;       valid users = MYDOMAIN\%S
```

Configuració en el hostpam

/etc/security/pam_mount.conf.xml

```
<volume user="*" fstype="cifs" server="samba" path="%(USER)"  mountpoint="~/%(USER)"
/>
```

Exemple en el hostpam

```
[root@host docker]# su - local01

[local01@host ~]$ su - anna
pam_mount password:

[anna@host ~]$ ll
total 0
drwxr-xr-x+ 2 anna alumnes 0 Dec 14 20:27 anna

[anna@host ~]$ mount -t cifs
//samba2/anna on /tmp/home/anna/anna type cifs
(rw,relatime,vers=1.0,cache=strict,username=anna,domain=,uid=5002,forceuid,gid=600,force
gid,addr=172.21.0.2,unix,posixpaths,serverino,mapposix,acl,rsize=1048576,wsize=65536,ech
o_interval=60,actimeo=1)
```

Exemple en el hostpam

```
#! /bin/bash
# @edt ASIX M06 2018-2019
# instal.lacio
# Creacio usuaris locals
```

```
groupadd localgrp01
groupadd localgrp02
useradd -g users -G localgrp01 local01
useradd -g users -G localgrp01 local02
useradd -g users -G localgrp01 local03
useradd -g users -G localgrp02 local04
useradd -g users -G localgrp02 local05
useradd -g users -G localgrp02 local06
echo "local01" | passwd --stdin local01
echo "local02" | passwd --stdin local02
echo "local03" | passwd --stdin local03
echo "local04" | passwd --stdin local04
echo "local05" | passwd --stdin local05
echo "local06" | passwd --stdin local06

# Activar nscd, nslcd, nsswitch  (lligar getent amb lsap)
#bash /opt/docker/auth.sh
cp /opt/docker/nslcd.conf /etc/nslcd.conf
cp /opt/docker/ldap.conf /etc/openldap/ldap.conf
cp /opt/docker/nsswitch.conf /etc/nsswitch.conf
#cp /opt/docker/system-auth-edt /etc/pam.d/system-auth-edt
#cp /opt/docker/pam_mount.conf.xml /etc/security/pam_mount.conf.xml
#ln -sf /etc/pam.d/system-auth-edt /etc/pam.d/system-auth
/usr/sbin/nslcd && echo "nslcd Ok"
/usr/sbin/nscd && echo "nscd Ok"

# Crear els homes dels usuaris de LDAP (crear-omplir-chown)
mkdir /tmp/home
mkdir /tmp/home/pere
mkdir /tmp/home/pau
mkdir /tmp/home/anna
mkdir /tmp/home/marta
mkdir /tmp/home/jordi
mkdir /tmp/home/admin

cp README.md /tmp/home/pere
cp README.md /tmp/home/pau
cp README.md /tmp/home/anna
cp README.md /tmp/home/marta
cp README.md /tmp/home/jordi
cp README.md /tmp/home/admin

chown -R pere.users /tmp/home/pere
chown -R pau.users /tmp/home/pau
chown -R anna.alumnes /tmp/home/anna
chown -R marta.alumnes /tmp/home/marta
chown -R jordi.users /tmp/home/jordi
```

```
chown -R admin.wheel /tmp/home/admin

# Generar dos directoris de shares samba d'exemple: public i privat
mkdir /var/lib/samba/public
chmod 777 /var/lib/samba/public
cp /opt/docker/* /var/lib/samba/public/.

mkdir /var/lib/samba/privat
#chmod 777 /var/lib/samba/privat
cp /opt/docker/smb.conf /etc/samba/smb.conf
cp /opt/docker/*.md /var/lib/samba/privat/.

# Usuaris locals super3 unix i samba
useradd patipla
useradd lila
useradd roc
useradd pla

echo -e "patipla\npatipla" | smbpasswd -a patipla
echo -e "lila\nlila" | smbpasswd -a lila
echo -e "roc\nroc" | smbpasswd -a roc
echo -e "pla\npla" | smbpasswd -a pla

# Crear els comptes Samba dels usuaris LDAP
echo -e "pere\npere" | smbpasswd -a pere
echo -e "pau\npau" | smbpasswd -a pau
echo -e "anna\nanna" | smbpasswd -a anna
echo -e "marta\nmarta" | smbpasswd -a marta
echo -e "jordi\njordi" | smbpasswd -a jordi
echo -e "admin\nadmin" | smbpasswd -a admin
```

En resum:

- Cal disposar d'usuaris unix (locals o de LDAP)
- En base als usuaris unix es creen els de SAMBA (el nom es el que fa el lligam al UID de unix).
- Cal crear els homes dels usaris LDAP (no en tenen) i assignar apropiadament el propietari i grup.
- Et voilà!