
RA6 — Integració de sistemes operatius lliures i propietaris

Índex

1. Per què cal la interoperabilitat	1
2. Serveis que permeten compartir recursos en xarxa	1
2.1. SMB/CIFS (Samba)	2
2.2. NFS	2
2.3. Impressió (CUPS / IPP)	2
3. Nivells de seguretat en l'accés als recursos compartits	2
3.1. Autenticació: qui ets	2
3.2. Autorització: què pots fer	3
3.3. Mapatge d'identitats en entorns heterogenis	3
3.4. Xifratge en trànsit	3
4. Comprovació de connectivitat en un escenari heterogeni	4
4.1. Escenari del laboratori	4
4.2. Nivells de comprovació (de baix a alt)	4
4.3. Ordres de comprovació típiques	4
5. Unir un client Linux al domini Active Directory	5
6. Instal·lació i configuració de Samba com a servidor de fitxers de domini	5
6.1. Instal·lació	5
6.2. Unió com a servidor membre i compartició	5
6.3. Accedir-hi des de client Windows	6
6.4. Accedir-hi des de client Linux	6
7. Compartició de recursos amb NFS i impressió heterogènia	7
7.1. Servidor NFS (Linux) amb seguretat Kerberos	7
7.2. Impressió compartida entre SO	7
8. Comprovació del funcionament dels serveis instal·lats	8
9. Pràctica en grup: accés a fitxers i impressores des de diferents SO	8
10. Documentació de la configuració dels serveis	9

1. Per què cal la interoperabilitat

A qualsevol organització real conviuen sistemes operatius diferents: estacions de treball Windows per a ofimàtica, servidors Linux per a serveis d'infraestructura, portàtils macOS de direcció, tauletes Android... Cap empresa es pot permetre illes comunicades.

Motius pels quals cal compartir recursos entre SO diferents:

- **Cost i llicenciament:** Linux i eines lliures per a servidors (baix cost, control total del codi); Windows on l'ecosistema d'aplicacions d'escriptori ho exigeix.
- **Especialització:** alguns serveis són més madurs en un món que en l'altre (p. ex. Active Directory a Windows, o determinades eines d'anàlisi a Linux).
- **Migracions graduals:** rarament es canvia tot un parc informàtic d'un dia per l'altre; cal conviure durant mesos o anys.
- **Continuïtat de negoci:** fitxers i impressores han de ser accessibles independentment del SO client.

Els recursos que típicament cal compartir entre SO són:

1. **Sistemes de fitxers en xarxa** (documents, perfils, aplicacions).
2. **Impressores i cues d'impressió.**
3. **Autenticació i identitat** (un mateix usuari i contrasenya des de qualsevol SO).
4. **Serveis de xarxa bàsics** (DNS, DHCP) que han de respondre igual a tothom.

La clau de la interoperabilitat és que **el protocol de xarxa és el contracte comú**: mentre client i servidor parlin el mateix protocol (SMB/CIFS, NFS, IPP, LDAP, Kerberos...), el SO de cada extrem és irrellevant.

2. Serveis que permeten compartir recursos en xarxa

Servei	Protocol	Origen	Ús típic
Samba	SMB/CIFS	Lliure (implementa el protocol de Microsoft)	Compartir fitxers/impressores des de Linux cap a Windows i viceversa; també pot fer de controlador de domini AD
NFS	NFSv3/NFSv4	Nadiu Unix/Linux	Compartir fitxers entre sistemes Unix/Linux; Windows en té client opcional
CUPS + IPP	Internet Printing Protocol	Lliure	Servidor d'impressió multiplataforma
Winbind / SSSD	---	Lliure	Permet a un Linux autenticar usuaris contra un domini AD (Kerberos + LDAP)
Active Directory	Kerberos, LDAP, DNS, SMB	Propietari (Microsoft), però amb clients lliures	Director centralitzat d'identitats i polítiques

2.1. SMB/CIFS (Samba)

SMB (*Server Message Block*), també conegut per l'antic nom **CIFS**, és el protocol natiu de compartició de fitxers i impressores de Windows. **Samba** és la implementació lliure d'aquest protocol per a sistemes Unix/Linux, i permet:

- Fer que un Linux actuï com a **servidor de fitxers** per a clients Windows (i Linux/macOS).
- Fer que un Linux s'uneixi a un **domini Active Directory** com a membre (o fins i tot com a controlador de domini, com al laboratori THOS.LOCAL).
- Que un client Linux **munti** un recurs compartit servit per un Windows Server.

2.2. NFS

Network File System és el protocol de compartició de fitxers natiu del món Unix. NFSv4 incorpora Kerberos per a autenticació segura, cosa que en facilita la integració amb AD. Windows disposa d'un component opcional (*Client for NFS / Server for NFS*) per interoperar-hi, tot i que a la pràctica és molt més habitual fer servir SMB quan hi ha Windows involucrat.

2.3. Impressió (CUPS / IPP)

CUPS (*Common Unix Printing System*) gestiona la impressió a Linux i pot exposar cues via **IPP**, el mateix protocol que fan servir nadiuament Windows i macOS des de fa anys. Alternativament, Samba pot compartir cues CUPS via SMB perquè els clients Windows les vegin com una impressora de xarxa clàssica.

3. Nivells de seguretat en l'accés als recursos compartits

Compartir un recurs sense controlar-ne l'accés és un risc de seguretat greu. Cal distingir diverses capes:

3.1. Autenticació: qui ets

- **Usuaris locals de Samba** (`smbpasswd`), independents del sistema: vàlid per a escenaris petits o standalone.
- **Usuaris de domini (Kerberos/AD)**: l'escenari recomanat en una xarxa heterogènia real. Un sol compte i una sola contrasenya serveixen per autenticar-se davant de qualsevol servei del domini THOS.LOCAL, sigui Windows o Linux.

3.2. Autorització: què pots fer

Cal distingir **dues capes de permisos independents** que sovint es confonen:

1. **Permisos de compartició (*share-level*)**: definits al servei (Samba valid users, read only, permisos NTFS de compartició a Windows). Determinen qui pot *arribar* al recurs per xarxa.
2. **Permisos del sistema de fitxers (*file-level*)**: ACL NTFS a Windows, o permisos POSIX/ACL POSIX (getfacl/setfacl) a Linux. Determinen què es pot fer un cop dins.

El permís efectiu és sempre **la intersecció més restrictiva de totes dues capes**. Per exemple, si la compartició Samba permet escriptura, però el permís POSIX del directori és r-x, l'usuari no podrà escriure.

3.3. Mapatge d'identitats en entorns heterogenis

Un dels reptes clàssics: un SID d'usuari de Windows/AD no és un UID Unix. Samba resol això amb idmap:

```
# /etc/samba/smb.conf (fragment, servidor membre de domini)
[global]
    workgroup = THOS
    realm = THOS.LOCAL
    security = ads

    idmap config * : backend = tdb
    idmap config * : range = 3000-7999
    idmap config THOS : backend = rid
    idmap config THOS : range = 10000-999999
```

Amb aquesta configuració, cada SID del domini THOS.LOCAL es tradueix de manera determinista a un UID/GID Linux, cosa que permet que els permisos POSIX reflecteixin la pertinença a grups d'AD (p. ex. Domain Users, Professors, Alumnes).

3.4. Xifratge en trànsit

- SMB3 xifra el trànsit per defecte quan client i servidor ho suporten (smb encrypt = desired/required a Samba).
- NFSv4 amb sec=krb5p xifra dades i autenticació.
- Cal evitar protocols antics sense xifrar (SMB1) o amb autenticació dèbil (NTLM sense signatura).

4. Comprovació de connectivitat en un escenari heterogeni

4.1. Escenari del laboratori

Reaprofitem la infraestructura THOS.LOCAL:

- **SRV-DC01**: controlador de domini (Samba AD-DC o Windows Server AD DS), amb DNS integrat.
- **SRV-FS01**: servidor de fitxers/impressió, membre del domini.
- **client-lin**: Debian/Ubuntu, membre del domini via sssd/winbind.
- **client-win**: Windows 10/11, membre del domini.

4.2. Nivells de comprovació (de baix a alt)

Nivell	Eina Linux	Eina Windows	Què verifica
Xarxa (ICMP)	ping, traceroute	ping, tracert	Encaminament bàsic
DNS	dig, nslookup, host	nslookup, Resolve-DnsName	Resolució del domini i registres SRV d'AD
Ports/serveis	nmap, nc -vz	Test-NetConnection	Ports oberts (445 SMB, 389/636 LDAP, 88 Kerberos, 53 DNS)
Aplicació	smbclient -L, showmount -e	net view, exploració xarxa	El servei respon i llista recursos

4.3. Ordres de comprovació típiques

```
# Des del client Linux, cap al DC
dig SRV-DC01.thos.local
dig -t SRV _ldap._tcp.thos.local
nc -vz SRV-DC01.thos.local 88      # Kerberos
nc -vz SRV-FS01.thos.local 445    # SMB

# Llistar recursos compartits d'un servidor Windows sense
↪ autenticar-se encara
smbclient -L //SRV-FS01.thos.local/ -U THOS\ramon
```

```
# Des del client Windows, cap al servidor Linux amb Samba
Test-NetConnection SRV-LINUX.thos.local -Port 445
nslookup SRV-DC01.thos.local
net view \\SRV-LINUX
```

NOTA

Si `smbclient -L` demana contrasenya i respon amb la llista de comparticions (IPC\$, comparticions creades), la capa d'aplicació SMB funciona correctament de cap a cap, incloent-hi l'autenticació.

5. Unir un client Linux al domini Active Directory

Pas previ imprescindible per treballar amb identitats de domini des de Linux.

```
sudo apt update
sudo apt install realmd sssd sssd-tools libnss-sss libpam-sss adcli
↪ samba-common-bin krb5-user

# Descobrir el domini
sudo realm discover thos.local

# Unir-se al domini (cal un compte amb privilegis d'unió)
sudo realm join --user=administrador thos.local

# Comprovar
realm list
id THOS\\ramon
getent passwd "THOS\\ramon"
```

Perquè els usuaris de domini puguin fer login interactiu, cal assegurar-se que pam_mkhome crea el directori d'inici automàticament:

```
sudo pam-auth-update --enable mkhomedir
```

6. Instal·lació i configuració de Samba com a servidor de fitxers de domini

6.1. Instal·lació

```
sudo apt install samba winbind libpam-winbind libnss-winbind
```

6.2. Unió com a servidor membre i compartició

```
# /etc/samba/smb.conf
[global]
    workgroup = THOS
    realm = THOS.LOCAL
    security = ads
    winbind use default domain = yes
    winbind refresh tickets = yes
    template shell = /bin/bash
    template homedir = /home/%U

    idmap config * : backend = tdb
    idmap config * : range = 3000-7999
```

```

idmap config THOS : backend = rid
idmap config THOS : range = 10000-999999

[dades]
  path = /srv/samba/dades
  valid users = @"THOS\Domain Users"
  read only = no
  browseable = yes
  force group = "THOS\Domain Users"
  create mask = 0660
  directory mask = 0770

[professors]
  path = /srv/samba/professors
  valid users = @"THOS\Professors"
  read only = no
  browseable = yes

```

```

sudo net ads join -U administrador
sudo systemctl restart smbd nmbd winbind
sudo systemctl enable smbd nmbd winbind

# Permisos POSIX del recurs
sudo mkdir -p /srv/samba/dades /srv/samba/professors
sudo chgrp "THOS\Domain Users" /srv/samba/dades
sudo chmod 2770 /srv/samba/dades

```

6.3. Accedir-hi des de client Windows

Des de l'explorador d'arxius de Windows: \\SRV-LINUX.thos.local\dades. Com que el client i el servidor comparteixen domini AD, l'autenticació és transparent (SSO amb Kerberos) si l'usuari ja ha iniciat sessió al domini.

6.4. Accedir-hi des de client Linux

```

# Muntatge manual amb credencials de domini (Kerberos)
sudo mount -t cifs //SRV-FS01.thos.local/documents /mnt/documents \
-o sec=krb5,cuid=$(id -u),multiuser

# Muntatge amb usuari/contrasenya (menys recomanable, sense SSO)
sudo mount -t cifs //SRV-FS01.thos.local/documents /mnt/documents \
-o username=ramon,domain=THOS,vers=3.1.1

# Entrada permanent a /etc/fstab
//SRV-FS01.thos.local/documents /mnt/documents cifs
↪ credentials=/root/.smbcreds,vers=3.1.1,uid=1000,gid=1000 0 0

```

7. Compartició de recursos amb NFS i impressió heterogènia

7.1. Servidor NFS (Linux) amb seguretat Kerberos

```
sudo apt install nfs-kernel-server
```

```
# /etc/exports
/srv/nfs/comu 10.0.10.0/24(rw, sync, sec=krb5, no_subtree_check)
```

```
sudo exportfs -ra
sudo systemctl restart nfs-kernel-server
```

Muntatge des d'un altre Linux:

```
sudo mount -t nfs4 -o sec=krb5 SRV-LINUX.thos.local:/comu /mnt/comu
```

NOTA

Windows només munta NFS amb el component opcional *Client for NFS* (edicions Pro/Enterprise), i sol requerir un mapatge d'usuaris addicional (NFS no coneix SID). Per aquest motiu, en un entorn amb Windows és preferible SMB per a la compartició principal i reservar NFS per a la interoperabilitat entre servidors Linux.

7.2. Impressió compartida entre SO

```
sudo apt install cups
sudo usermod -aG lpadmin ramon
sudo systemctl enable --now cups
```

Afegir la impressora via la interfície web de CUPS (<https://localhost:631>) i, per exposar-la també via SMB als clients Windows:

```
# /etc/samba/smb.conf
[printers]
comment = Totes les impressores
path = /var/spool/samba
browseable = no
printable = yes
guest ok = no
```

```
sudo mkdir -p /var/spool/samba
sudo chmod 1777 /var/spool/samba
sudo systemctl restart smbd cups
```

Des de Windows: \\SRV-LINUX.thos.local mostrarà la impressora com un recurs més, instal·lable amb el driver corresponent.

Des de Linux/macOS es pot afegir directament via IPP: `ipp://SRV-LINUX.thos.local:631/printers/nom_impessora`.

8. Comprovació del funcionament dels serveis instal·lats

Comprovació	Ordre
Sintaxi de <code>smb.conf</code> vàlida	<code>testparm</code>
Unió al domini correcta	<code>net ads testjoin</code>
Tiquet Kerberos vigent	<code>klist</code>
Resolució d'identitats de domini	<code>wbinfo -u,wbinfo -g,id THOS\usuari</code>
Sessions SMB actives	<code>smbstatus</code>
Comparticions visibles	<code>smbclient -L localhost -U%</code>
Exports NFS actius	<code>showmount -e localhost</code>
Cues d'impressió	<code>lpstat -p -d</code>
Registre d'errors	<code>journalctl -u smbd -u winbind -f</code>

```
testparm -s
net ads testjoin
wbinfo -t
smbstatus
showmount -e localhost
lpstat -p -d
```

Un servei es considera “verificat” quan es compleixen **tres condicions**: el dimoni està actiu (`systemctl status`), respon localment (ordres anteriors) i és accessible des d'un client de l'altre SO amb les credencials i permisos previstos.

9. Pràctica en grup: accés a fitxers i impressores des de diferents SO

Repartiment de rols suggerit:

1. **Rol servidor:** configura Samba (§6) i CUPS+Samba (§7.2) al servidor comú, defineix grups d'AD (Professors, Alumnes) i n'assigna permisos diferenciats a dues comparticions.
2. **Rol client Windows:** es connecta a les comparticions, verifica que el SSO funciona amb l'usuari de domini, imprimeix un document de prova a la impressora compartida.
3. **Rol client Linux:** uneix la seva màquina al domini (§5), munta les comparticions per CIFS (§6.4), imprimeix via IPP a la mateixa impressora.

Lliurable de la pràctica:

- Captura de pantalla de cada client accedint correctament al recurs.
- Prova que un usuari del grup Alumnes **no** pot escriure a la compartició professors (evidència del control d'accés).
- Un document imprès (o el PDF generat per una impressora virtual) des de cada SO.

10. Documentació de la configuració dels serveis

Documentar no és opcional: sense documentació, cap configuració és mantenible ni auditable. Cada servei desplegat ha d'anar acompanyat d'una fitxa amb, com a mínim:

```
## Fitxa de servei: Samba --- SRV-FS01

- Rol al domini: membre de THOS.LOCAL
- Versió: Samba x.x.x (Debian/Ubuntu xx.xx)
- Comparticions:
  | Nom          | Ruta                      | Grup autoritzat | Permisos |
  |-----|-----|-----|-----|
  | dades        | /srv/samba/dades         | Domain Users    | rw       |
  | professors   | /srv/samba/professors    | Professors      | rw       |
- Mapatge idmap: rid, rang 10000-999999 per a THOS
- Xifratge: smb encrypt = desired
- Dependències: DNS i Kerberos de SRV-DC01
- Còpia de seguretat: inclosa a la política de BackupPC (vegeu fitxa
  ↪ corresponent)
- Data última modificació / autor: ...
- Incidències conegudes: ...
```

Aquesta documentació ha de:

- Viure en un dipòsit versionat (o com a mínim en un sistema amb historial, com GLPI o una wiki).
- Incloure **el perquè**, no només el què (per exemple, per què s'ha triat rid i no autorid a l'idmap).
- Reflectir l'estat *real* del sistema, actualitzant-se en cada canvi de configuració.

Versions d'aquest document

- [HTML](#)
- [PDF](#)
- [ODT](#)
- [MD](#)

[Domini Públic \(CC0\)](#)