

Activitat LDAP (Part2): Integració amb SAMBA en LDAP

MÒDUL	GRUP:	QUALIFICACIÓ:
UF1 - RA1. Administra el servei de directori interpretant especificacions i integrant-lo en una xarxa.		
NOM I COGNOMS:	DATA:	

Part pràctica

Entorn

En aquesta pràctica integrareu **SAMBA** amb el servidor **LDAP** configurat a la pràctica anterior, permetent l'**autenticació centralitzada** i l'**accés a recursos compartits**. Configurareu el servidor per a que actui com a controlador de domini bàsic i provareu la connexió des d'un client Windows.

Objectius

1. Integrar Samba amb OpenLDAP
2. Gestionar autenticació i recursos compartits en una xarxa heterogènia.

Requisits previs

- Servidor LDAP funcional de la part 1.
- Una màquina client amb Windows (Client de RSAT)

Avaluació

- Un 15% de la nota d'aquesta activitat s'obtindrà a partir de l'entrega de l'activitat (5% cada part).
- El 85% restant s'obtindrà amb un petit test que es farà via Moodle.

Tasques a realitzar

Tasca 1: Preparació del Servidor:

1. Instal·la els paquets **samba**, **smbldap-tools**, **libnss-ldap** i **libpam-ldap**.

```
tsard@ubuntu-server:~$ sudo apt install samba smbldap-tools libnss-ldap libpam-ldap
```

Durant la instal·lació, s'obrirà un assistent on hem d'introduir les nostres dades.

Introduïm la IP del servidor per tal de formar la URL:

Configuració del paquet «ldap-auth-config»

Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>[:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.
Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.

LDAP server Uniform Resource Identifier:

ldap://192.168.0.254

<Ok>

Definim el domini:

Configuració del paquet «ldap-auth-config»

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=pepgarcia,dc=local

<Ok>

Seleccionem la versió 3, que ve per defecte:

Configuració del paquet «ldap-auth-config»

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3
2

<Ok>

La resta d'opcions, també amb el valor per defecte:

Configuració del paquet «ldap-auth-config»

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

☒ <Yes> ☐ <No>

No requerir login per fer consultes:

Configuració del paquet «ldap-auth-config»

Choose this option if you are required to login to the database to retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

☐ <Yes> ☒ <No>

Configurem les nostres dades:

Configuració del paquet «ldap-auth-config»

This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

Configurem la contrasenya: admin1234

Configuració del paquet «ldap-auth-config»

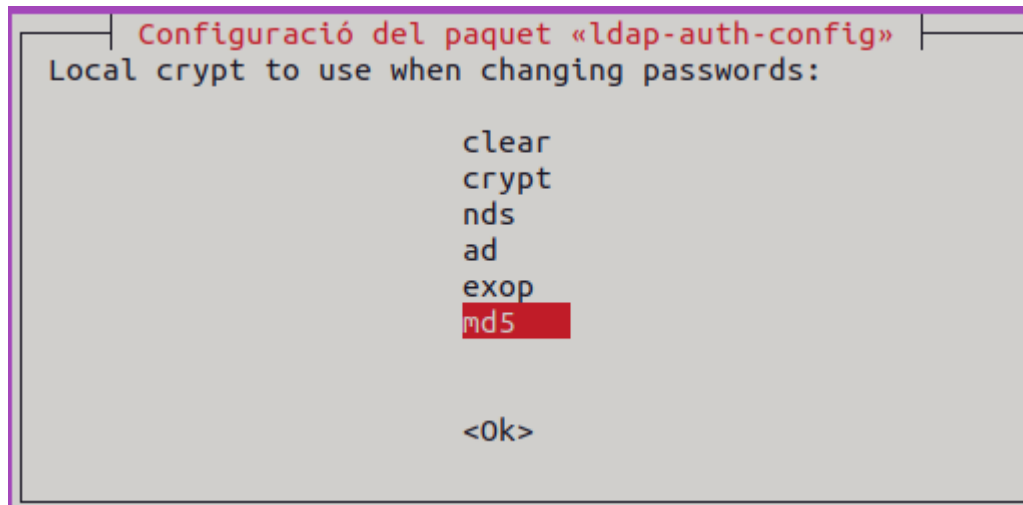
Please enter the password to use when ldap-auth-config tries to login to the LDAP directory using the LDAP account for root.

The password will be stored in a separate file /etc/ldap.secret which will be made readable to root only.

Entering an empty password will re-use the old password.

LDAP root account password:

Triem l'opció d'enciptació per defecte:



2. Configura **NSS** a **/etc/nsswitch.conf** per utilitzar LDAP a **passwd, group i shadow**.
NSS a LDAP permet al sistema operar amb usuaris i grups de LDAP com si fossin usuaris locals, facilitant la gestió centralitzada d'identitats en xarxes corporatives.

```
passwd:      files systemd sss ldap
group:       files systemd sss ldap
shadow:      files sss ldap
gshadow:     files
```

3. Configura **PAM** a **/etc/pam.d/common-session** per crear directoris d'usuari automàticament.

Per habilitar la creació automàtica cal afegir aquesta línia:

```
session optional pam_systemd.so
# end of pam-auth-update config
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

Tasca 2: Afegir Esquema Samba al LDAP:

1. Instal·la **samba-doc** i copia el fitxer **samba.schema.gz** a **/etc/ldap/schema/**.
2. Descomprimeix el fitxer i converteix-lo a LDIF usant un fitxer de configuració temporal (**schema_convert.conf**) i la comanda **slapcat**.
3. Edita el fitxer LDIF generat per eliminar índexs i metadades innecessàries.
4. Afegeix l'esquema al directori amb **ldapadd**.

Com que no trobem el **samba-doc**, baixem un **samba.ldif** ja muntat:

```
lsard@ubuntu-server:~$ wget https://raw.githubusercontent.com/zentyal/samba/refs/heads/master/examples/LDAP/samba.ldif -O samba.ldif
--2025-03-21 18:33:21-- https://raw.githubusercontent.com/zentyal/samba/refs/heads/master/examples/LDAP/samba.ldif
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)[185.199.111.133]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14892 (15K) [text/plain]
Saving to: 'samba.ldif'

samba.ldif
100%[=====]
2025-03-21 18:33:21 (65,3 MB/s) - 'samba.ldif' saved [14892/14892]
```

I l'afegim al directori:

```
isard@ubuntu-server:~$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f samba.ldif
[sudo] password for isard:
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=samba,cn=schema,cn=config"
```

Definim els nous índexs:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

Afegim els nous índex a la base de dades:

```
isard@ubuntu-server:~$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f samba_indexes.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}hdb,cn=config"
ldap_modify: No such object (32)
    matched DN: cn=config
```

Tasca 3: Configuració de Samba:

Editor /etc/samba/smb.conf amb les següents opcions:

1. **workgroup = NomCognom**
2. **netbios name = SERVIDOR**
3. **security = user**
4. **passdb backend = ldapsam:ldap://localhost**
5. **ldap admin dn = cn=admin,dc=nomcognom,dc=local**
6. **ldap suffix = dc=nomcognom,dc=local**
7. **ldap user suffix = ou=Professors**
8. **ldap group suffix = ou=Professors**
9. **ldap machine suffix = ou=Ordinadors**

10. ldap ssl = no

He afegit després del workgroup, que ja estava al fitxer, la resta de camps:

```
# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = PepGarcia
netbios name = SERVIDOR
security = user
passdb backend = ldapsam:ldap://localhost
ldap admin dn = cn=admin,dc=pepgarcia,dc=local
ldap suffix = dc=pepgarcia,dc=local
ldap user suffix = ou=Profesors
ldap group suffix = ou=Professors
ldap machine suffix = ou=Ordinadors
ldap ssl = no
```

Encara que no ho diu, podem comprovar que la sintaxi és correcta amb testparm:

```
isard@ubuntu-server:~$ sudo testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions
```

Reinicieu Samba i afegiu la contrasenya de l'administrador amb **smbpasswd -W**.

Primer cal afegir la contrasenya perquè si no, es produeix un error al reiniciar:

```
isard@ubuntu-server:~$ sudo smbpasswd -w admin1234
Setting stored password for "cn=admin,dc=pepgarcia,dc=local" in secrets.tdb
isard@ubuntu-server:~$ sudo systemctl restart smbd.service
isard@ubuntu-server:~$ sudo systemctl status smbd.service
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-03-26 18:05:33 UTC; 24s ago
     Press q to quit / ? for help
```

Afegeix un recurs compartit [recursos] a **/srv/samba/recursos** amb permisos d'escriptura.

Editem els fitxer **/etc/samba/smb.conf** i afegim l'apartat recursos. És important fer-ho al final per a que no es produisca cap error:

```
[recursos]
path = /srv/samba/recursos
writable = yes
read only = no
browsable = yes
```

Reiniciem el servei i comprovem que segueix funcionant correctament:

```
isard@ubuntu-server:~$ sudo systemctl restart smbd.service
isard@ubuntu-server:~$ sudo systemctl status smbd.service
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-03-26 19:23:53 UTC; 4s ago
     Docs: man:smbd(8)
           man:samba(7)
```

Tasca 4: Prova d'integració:

1. Afegiu l'usuari "professor1" com a usuari Samba amb **smbldap-useradd** i configura la contrasenya.

Si ho fem directament, es produirà un error ja que abans hem de configurar correctament les utilitats smbldap-tools.

```
isard@ubuntu-server:~$ smbldap-useradd -a -m -u 2001 professor1
Unable to open /etc/smbldap-tools/smbldap.conf for reading !
Compilation failed in require at /usr/sbin/smbldap-useradd line 29.
BEGIN failed--compilation aborted at /usr/sbin/smbldap-useradd line 29.
```

Creem el fitxer smbldap.conf amb la nostra informació. Aquest fitxer defineix la connexió de Samba amb el servidor LDAP i com es gestionen els usuaris i grups.

```
GNU nano 6.2 /etc/smbldap-tools/smbldap.conf *
#####
# Configuració bàsica de smbldap-tools
#####

# URL del servidor LDAP
ldapserver="ldap://localhost"

# Si tens un servidor esclau de LDAP, pots afegir-lo aquí
#ldapbackup="ldap://backup.example.com"

# Base DN del directori LDAP
suffix="dc=pepgarcia,dc=local"

# DN de l'administrador LDAP (ha de coincidir amb `smbldap_bind.conf`)
ldapadmin="cn=admin,dc=pepgarcia,dc=local"

# DN on es troben els usuaris
usersdn="ou=Usuaris,${suffix}"

# DN on es troben els grups
groupsdn="ou=Grups,${suffix}"

# DN on es troben els ordinadors
computersdn="ou=Ordinadors,${suffix}"

# DN on es troben els dominis
ldmapdn="ou=Dominis,${suffix}"

# Habilitar TLS (si es vol utilitzar SSL)
ldapssl="no"

# DN del domini Samba (només si fas servir control de dominis)
#sambaDomain="EXAMPLEDOMAIN"
```

Creem el fitxer smbldap_bind.conf. Aquest fitxer conté les credencials per permetre que smbldap-tools accedeixi al directori LDAP.


```
GNU nano 6.2 /etc/smbldap-tools/smbldap_bind.conf
# DN de l'usuari administrador LDAP (ha de coincidir amb `smbldap.conf`)
binddn="cn=admin,dc=pepgarcia,dc=local"

# Contrasenya de l'usuari administrador LDAP
bindpw=admin1234

# Si fas servir TLS per connectar-te a LDAP
masterLDAP="ldap://localhost"
#slaveLDAP="ldap://backup.example.com"

# Activa TLS si el servidor LDAP l'exigeix
verify="require"
cafile="/etc/ssl/certs/ca-certificates.crt"
```

El fitxer smbldap_bind.conf conté la contrasenya de l'usuari LDAP, per la qual cosa cal restringir-ne els permisos:

```
isard@ubuntu-server:~$ sudo chmod 600 /etc/smbldap-tools/smbldap_bind.conf
isard@ubuntu-server:~$ sudo chown root:root /etc/smbldap-tools/smbldap_bind.conf
```

Finalment, ja podem crear l'usuari:

```
isard@ubuntu-server:~$ sudo smbldap-useradd -a -m -u 2001 professor1
UID already owned by uid=professor1,ou=Professors,dc=pepgarcia,dc=local
isard@ubuntu-server:~$ sudo smbpasswd -a professor1
New SMB password:
Retype new SMB password:
Added user professor1.
```

2. Crea el directori compartit i reinicia Samba.

Creem el directori que hem definit al fitxer smb.conf, és a dir /srv/samba/recursos

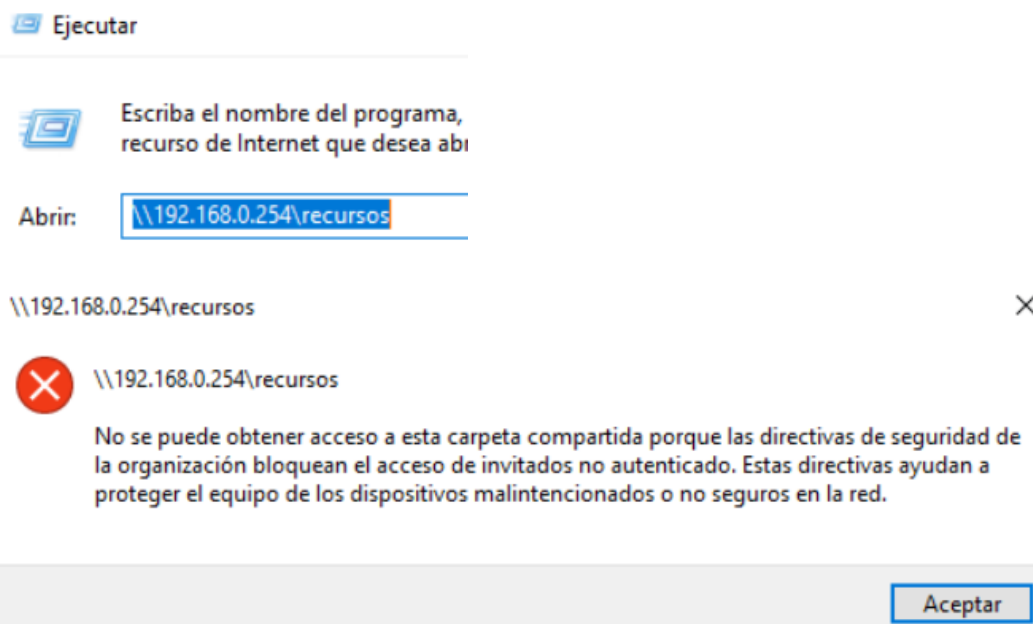
```
isard@ubuntu-server:~$ sudo mkdir -p /srv/samba/recursos
```

Després, reiniciem el servei i comprovem que tot està bé:

```
isard@ubuntu-server:~$ sudo systemctl restart smbd.service
isard@ubuntu-server:~$ sudo systemctl status smbd.service
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2025-03-27 11:51:23 UTC; 1min 1s ago
     Docs: man:smbd(8)
```

3. Connecta des d'un client Windows a \\<IP_DEL_SERVIDOR>\recursos amb les credencials de "professor1".

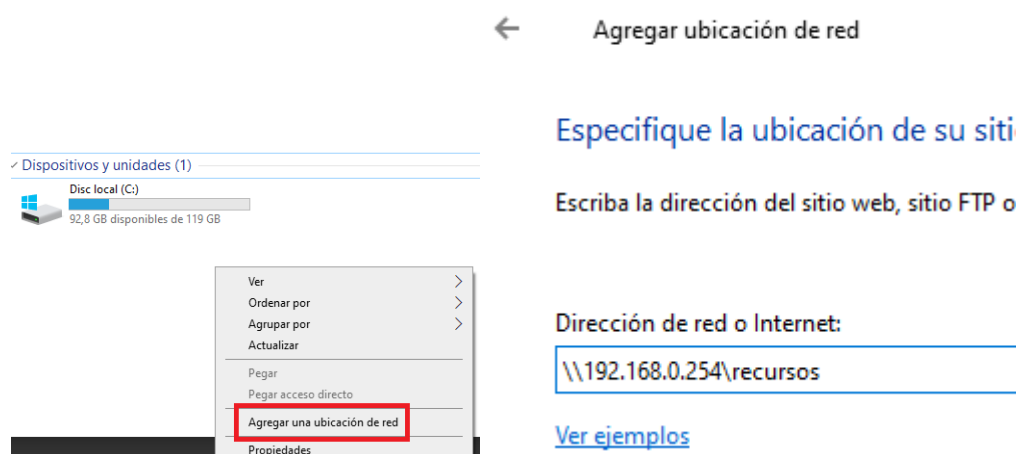
Si afegim la carpeta afegint directament una unitat de xarxa a l'explorador de fitxers o des de l'executar, no la troba i ens mostra el següent error:



Una solució és establir la connexió manualment amb “net use”, que s'utilitza per connectar, desconnectar i gestionar unitats de xarxa compartides:

```
C:\Users\isard>net use \\192.168.0.254\recursos /user:pepgarcia\professor1
Escriba la contraseña de "pepgarcia\professor1" para conectar a "192.168.0.254":
Se ha completado el comando correctamente.
```

Un cop establerta la connexió, afegim una unitat:



Agregar ubicación de red

¿Qué nombre le desea dar a esta ubicación?

Dé un nombre a este acceso directo que le permita identificar con facilidad.

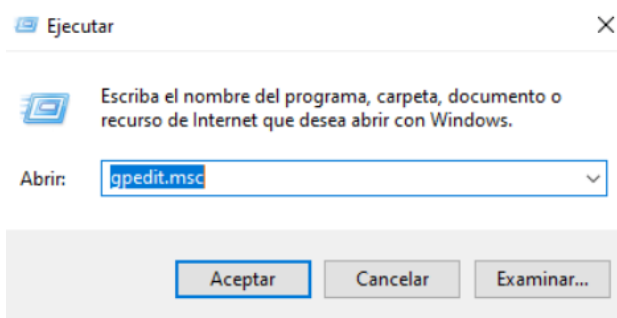
\\192.168.0.254\recursos.

Escriba un nombre para esta ubicación de red:

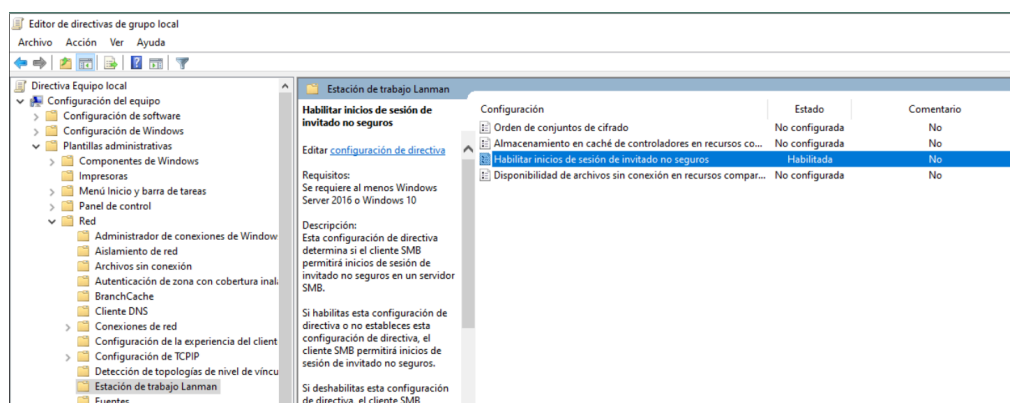
recursos (192.168.0.254 (ubuntu-server server (Samba, Ubuntu)))

Aquesta solució però, implica que cada cop que reiniciem, haguem de tornar a establir connexió. Si volem que ens demane les credencials quan intentem connectar, hem de modificar la directiva de seguretat de Windows:

Obrim l'editor de directives locals:



I activem la directiva Configuració d'equip → Plantilles administratives → Xarxa → Estació de treball Lanman:



Un cop activada al intentar accedir ja ens demana automàticament les credencials:

