
RA1. Administració del servei de directori

Índex

Introducció	1
1. Funció, elements i estructures lògiques del servei de directori	1
1.1. Què és i per a què serveix	1
1.2. Model de dades LDAP: el DIT	2
1.3. LDAP com a protocol	3
2. Esquema del servei de directori	3
2.1. Components de l'esquema	3
2.2. Esquema en OpenLDAP	3
2.3. Esquema en Active Directory / Samba AD DC	4
3. Controladors de domini	4
3.1. Característiques	4
3.2. Topologia de laboratori	4
4. Instal·lació del servei de directori	5
4.1. Requisits previs	5
4.2. Aprovisionament del domini	5
4.3. Activar i verificar el servei	6
5. Configuració i personalització del servei de directori	6
5.1. Estructura d'unitats organitzatives (OU)	6
5.2. Política de contrasenyes i seguretat	7
5.3. Personalització de l'esquema (avançat)	7
6. Integració amb altres serveis	7
7. Filtres de cerca en el servei de directori	8
7.1. Sintaxi bàsica	8
7.2. Exemples pràctics amb ldapsearch	8
8. Autenticació centralitzada d'usuaris	9
9. Configuració del client per a la integració en el domini	10
9.1. Client Windows	10
9.2. Client Linux amb SSSD	10
10. Eines gràfiques i ordres per a l'administració	11
10.1. Ordres (Samba AD DC)	11
10.2. Eines gràfiques	11
11. Documentació de l'estructura i la implantació	11

Cicle: Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0374. Administració de sistemes operatius

Introducció

Un **servei de directori** és una base de dades jeràrquica especialitzada, optimitzada per a operacions de lectura i cerca, que emmagatzema informació sobre els recursos d'una xarxa: usuaris, grups, equips, impressores, polítiques de seguretat, etc. És l'element central que permet gestionar de manera **centralitzada** l'autenticació i l'autorització en una xarxa corporativa.

En aquest document treballarem els dos estàndards que trobareu en qualsevol organització:

- **LDAP (Lightweight Directory Access Protocol)**, el protocol i el model de dades sobre el qual es construeixen la majoria de serveis de directori.
- **Active Directory (AD)**, la implementació de Microsoft, que ampliem amb **Samba AD DC**, la implementació lliure compatible que farem servir al nostre laboratori (domini TH0S.LOCAL).

NOTA

Tot i que Active Directory i Samba AD DC ofereixen eines pròpies (com `samba-tool` o els complements RSAT), per sota totes dues implementacions parlen LDAP i Kerberos. Entendre LDAP és la clau per entendre qualsevol servei de directori, sigui quin sigui el fabricant.

1. Funció, elements i estructures lògiques del servei de directori

1.1. Què és i per a què serveix

El servei de directori resol un problema molt concret: en una xarxa amb desenes o milers d'equips i usuaris, no és viable gestionar comptes i permisos equip per equip. El directori centralitza aquesta informació i l'ofereix a qualsevol servei de la xarxa (fitxers, correu, VPN, aplicacions) mitjançant un protocol comú.

Funcions principals:

- **Autenticació centralitzada:** un sol compte i una sola contrasenya per accedir a tots els recursos (*single sign-on*).
- **Autorització:** control de qui pot accedir a què, mitjançant grups i polítiques.
- **Localització de recursos:** cerca d'usuaris, equips, impressores, etc.
- **Gestió centralitzada:** aplicació de polítiques (GPO en AD) des d'un punt únic.

1.2. Model de dades LDAP: el DIT

LDAP organitza la informació en un arbre anomenat **DIT (Directory Information Tree)**. Cada node de l'arbre és una **entrada (entry)**, identificada de manera única per un **DN (Distinguished Name)**.

```
dc=thos,dc=local
├── ou=Usuaris
│   ├── cn=jperez
│   └── cn=mgarcia
├── ou=Grups
│   └── cn=Professorat
├── ou=Equips
│   └── cn=PC-AULA01
└── cn=Users (contenidor per defecte, en AD)
```

Elements bàsics del model:

Element	Descripció	Exemple
Entry	Un objecte del directori (usuari, grup...)	cn=jperez,ou=Usuaris,dc=thos,dc=local
DN	Camí complet i únic d'una entrada	cn=jperez,ou=Usuaris,dc=thos,dc=local
RDN	La part del DN pròpia de l'entrada (relative DN)	cn=jperez
Atribut	Parella clau-valor dins d'una entrada	mail: jperez@thos.local
objectClass	Defineix quins atributs pot/ha de tenir l'entrada	person, organizationalUnit
OU	<i>Organizational Unit</i> , contenidor lògic dins l'arbre	ou=Professorat

Nomenclatura habitual d'atributs (RDN):

Abreviatura	Significat
dc	Domain Component (component del domini, ex. dc=thos, dc=local)
ou	Organizational Unit
cn	Common Name
sn	Surname (cognom)
uid	User ID
dn	Distinguished Name (el camí sencer, no és un atribut d'entrada pròpiament)

1.3. LDAP com a protocol

LDAP defineix també les operacions que un client pot fer contra el directori:

- **bind** --- autenticar-se davant el servidor.
- **search / compare** --- cercar i comparar entrades.
- **add / delete / modify** --- crear, esborrar i modificar entrades.
- **unbind** --- tancar la sessió.

El port estàndard és el **389/TCP** (LDAP en text pla, normalment protegit amb **STARTTLS**) i el **636/TCP** per a **LDAPS** (LDAP sobre SSL/TLS de forma nativa).

2. Esquema del servei de directori

L'**esquema** és el conjunt de regles que defineixen quins tipus d'objectes (**objectClass**) poden existir al directori i quins atributs pot o ha de tenir cadascun. Sense esquema, LDAP no sabia si un atribut és vàlid ni de quin tipus de dada es tracta.

2.1. Components de l'esquema

- **objectClass**: defineix una "plantilla" d'objecte. Poden ser:
 - **STRUCTURAL**: defineix la naturalesa bàsica de l'entrada (una entrada només en pot tenir un). Ex.: `inetOrgPerson`, `organizationalUnit`.
 - **AUXILIARY**: afegeix atributs opcionals a una entrada ja definida per una classe estructural. Ex.: `posixAccount`.
 - **ABSTRACT**: classes base de les quals n'hereten altres (ex. `top`).
- **Atributs (attributeType)**: cada atribut té un OID únic, un tipus de sintaxi (cadena, enter, binari...) i pot ser d'un sol valor o multivaluat.
- **Herència**: les **objectClass** es defineixen jeràrquicament (ex. `inetOrgPerson` hereta de `organizationalPerson`, que hereta de `person`, que hereta de `top`).

2.2. Esquema en OpenLDAP

A OpenLDAP l'esquema es defineix en fitxers `.schema` o `.ldif` (a `cn=schema,cn=config`). Es poden inspeccionar amb:

```
ldapsearch -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config -s one dn
```

2.3. Esquema en Active Directory / Samba AD DC

En AD, l'esquema es defineix a la partició CN=Schema, CN=Configuration, DC=thos, DC=local i és **comú a tot el bosc** (forest). Ampliar-lo (per exemple per afegir atributs propis d'una aplicació) és una operació irreversible i s'ha de fer amb molta cura.

Es pot consultar amb `samba-tool`:

```
samba-tool schema attribute list
samba-tool schema objectclass list
```

NOTA

A diferència d'OpenLDAP, on cada organització sovint defineix el seu propi esquema “des de zero” combinant .schema estàndard, a Active Directory l'esquema ja ve predefinit amb centenars de classes (usuari, equip, grup, GPO...) i normalment no cal tocar-lo.

3. Controladors de domini

Un **controlador de domini (DC)** és el servidor que allotja una còpia (parcial o completa) de la base de dades del directori i que respon a les peticions d'autenticació i consulta.

3.1. Característiques

- Un domini pot tenir **més d'un DC** per redundància i repartiment de càrrega.
- Els DC es **reliquen** entre ells de manera multi-mestre (Active Directory / Samba AD DC): tots els DC poden acceptar canvis i després es propaguen.
- Cada DC sol assumir també el rol de **servidor DNS** integrat, ja que els clients localitzen els DC mitjançant registres SRV al DNS (`_ldap._tcp.thos.local`, `_kerberos._tcp.thos.local`).
- En entorns AD hi ha rols especials anomenats **FSMO** (Flexible Single Master Operations) que, tot i la replicació multi-mestre, s'assignen a un únic DC per evitar conflictes (ex. *PDC Emulator*, *RID Master*).

3.2. Topologia de laboratori

En un entorn de pràctiques típic (com el nostre laboratori amb SRV-DC01 i SRV-FS01), és habitual desplegar **dos controladors de domini** per estudiar:

- La replicació de la base de dades del directori.
- La tolerància a fallades (què passa si un DC cau).
- El comportament del DNS integrat en un escenari multi-DC.

THOS.LOCAL





4. Instal·lació del servei de directori

Farem la instal·lació amb **Samba AD DC**, que nosaltres proveïm com a primer controlador d'un domini nou (THOS.LOCAL) sobre Debian/Ubuntu Server.

4.1. Requisits previs

- Nom de màquina resolt correctament (FQDN).
- **Hora sincronitzada** (Kerberos és molt sensible al desfasament horari; cal NTP/chrony actiu).
- Cap altre servei de DNS o Samba escoltant als ports necessaris.

```
sudo hostnamectl set-hostname srv-dc01.thos.local
sudo apt update
sudo apt install samba krb5-config krb5-user winbind smbclient chrony
↵ -y
```

4.2. Aprovisionament del domini

```
sudo systemctl stop smbd nmbd winbind
sudo systemctl disable smbd nmbd winbind

sudo samba-tool domain provision \
  --use-rfc2307 \
  --realm=THOS.LOCAL \
  --domain=THOS \
  --server-role=dc \
  --dns-backend=SAMBA_INTERNAL \
  --adminpass='ContrasenyaSegura1!'
```

Paràmetres clau:

- `--realm`: nom complet del regne Kerberos / domini DNS (en majúscules per convenció).
- `--domain`: nom NetBIOS curt del domini.
- `--dns-backend=SAMBA_INTERNAL`: Samba fa també de servidor DNS, integrat amb el directori.
- `--use-rfc2307`: afegeix atributs POSIX (uid, gid...) a l'esquema, imprescindible per autenticar clients Linux.

4.3. Activar i verificar el servei

```
sudo systemctl unmask samba-ad-dc
sudo systemctl enable --now samba-ad-dc
sudo systemctl status samba-ad-dc
```

Verificacions bàsiques:

```
# Comprovar el DNS propi
host -t SRV _ldap._tcp.thos.local

# Comprovar Kerberos
sudo kinit administrator
klist

# Nivell funcional i informació del domini
samba-tool domain level show
```

AVÍS

Si kinit falla amb un error de tipus *clock skew*, revisa primer la sincronització horària (`chronyc tracking`) abans de sospitar de la configuració de Kerberos.

5. Configuració i personalització del servei de directori

Un cop desplegat, cal adaptar el directori a l'estructura de l'organització.

5.1. Estructura d'unitats organitzatives (OU)

Les OU permeten organitzar objectes i, sobretot, **aplicar polítiques (GPO) de manera diferenciada**. Una estructura típica d'institut:

```
THOS.LOCAL
├── OU=Professorat
│   ├── OU=SMX
│   └── OU=ASIX
├── OU=Alumnat
│   ├── OU=1r-ASIX
│   └── OU=2n-ASIX
├── OU=Equips
│   ├── OU=Aules
│   └── OU=Professorat
└── OU=Serveis
```

```
samba-tool ou create "OU=Professorat,DC=thos,DC=local"
samba-tool ou create "OU=SMX,OU=Professorat,DC=thos,DC=local"
samba-tool ou create "OU=Alumnat,DC=thos,DC=local"
```

```
samba-tool ou list
```

5.2. Política de contrasenyes i seguretat

```
samba-tool domain passwordsettings set --min-pwd-length=10
samba-tool domain passwordsettings set --complexity=on
samba-tool domain passwordsettings set --max-pwd-age=90
samba-tool domain passwordsettings show
```

5.3. Personalització de l'esquema (avançat)

Ampliar l'esquema (per exemple, afegir un atribut numExpedient als usuaris) es fa mitjançant fitxers **LDIF** aplicats amb privilegis d'administrador d'esquema. Es tracta d'una operació poc habitual i que **no té marxa enrere**, per la qual cosa cal documentar-la sempre abans d'aplicar-la (vegeu apartat 10).

6. Integració amb altres serveis

El valor real d'un directori està en la seva capacitat d'integrar-se amb altres serveis de xarxa perquè comparteixin una única font d'identitats.

Servei	Mecanisme d'integració
DNS	El mateix DC actua com a servidor DNS autoritatiu del domini (registres SRV, A, PTR).
Compartició de fitxers (Samba/CIFS)	Els recursos compartits validen l'accés contra el directori mitjançant Kerberos/NTLM.
Correu electrònic	Les llibretes d'adreces i l'autenticació SMTP/IMAP poden consultar LDAP.
VPN / xarxa (RADIUS)	FreeRADIUS pot delegar l'autenticació a LDAP o Kerberos.
Aplicacions web	Autenticació via LDAP bind o SAML/OIDC amb un IdP connectat al directori.
Linux (SSSD)	Els clients Linux autèntiquen i resolen usuaris/grups contra el directori (apartat 9).

Exemple: configurar una compartició Samba autenticada contra el mateix directori (en el mateix DC o en un membre de domini):

```
[documents]
  path = /srv/samba/documents
  valid users = @"THOS\Professorat"
  read only = no
```

NOTA

Aquesta capacitat d'integració és el que distingeix un "simple magatzem d'usuaris" d'un veritable servei de directori: el mateix compte jper ez serveix per iniciar sessió a l'equip, accedir a la carpeta compartida, connectar-se a la VPN i consultar el correu, sense haver

de duplicar credencials enlloc.

7. Filtres de cerca en el servei de directori

Les cerques LDAP es construeixen amb **filtres** que segueixen la sintaxi RFC 4515, basada en parèntesis i operadors booleans.

7.1. Sintaxi bàsica

Operador	Símbol	Exemple
Igual	=	(cn=jperez)
AND	&	(&(objectClass=user)(department=Informàtica))
OR		(\ (cn=jperez)(cn=mgarcia))
NOT	!	(!(userAccountControl:1.2.840.113556.1.4.803:=2))
Aproximat	~=	(sn~=Garcia)
Comodí	*	(cn=j*)
Presència	=*	(mail=*)

7.2. Exemples pràctics amb ldapsearch

```
# Tots els usuaris del departament d'Informàtica
ldapsearch -x -H ldap://srv-dc01.thos.local \
  -b "dc=thos,dc=local" \
  "(&(objectClass=user)(department=Informatica))" \
  cn mail

# Usuaris amb el compte deshabilitat (bit 2 de userAccountControl)
ldapsearch -x -H ldap://srv-dc01.thos.local -D
↳ "administrator@thos.local" -W \
  -b "dc=thos,dc=local" \
  "(userAccountControl:1.2.840.113556.1.4.803:=2)"

# Grups que contenen un usuari concret (regla de coincidència en
↳ cadena, memberOf)
ldapsearch -x -H ldap://srv-dc01.thos.local -D
↳ "administrator@thos.local" -W \
  -b "dc=thos,dc=local" \
  "(member:1.2.840.113556.1.4.1941:=cn=jperez,ou=Alumnat,dc=thos,dc=
↳ local)"
```

Equivalent amb `samba-tool`, sense necessitat de conèixer tota la sintaxi LDIF:

```
samba-tool user list
samba-tool group listmembers "Professorat"
```

8. Autenticació centralitzada d'usuaris

El directori actua com a **autoritat d'autenticació** per a tota la xarxa gràcies a dos mecanismes complementaris:

- **Bind LDAP simple:** el client envia usuari i contrasenya, i el servidor valida les credencials contra l'entrada corresponent. Senzill, però requereix xifrar el canal (TLS) perquè la contrasenya no viatgi en text pla.
- **Kerberos:** protocol d'autenticació basat en tiquets, on la contrasenya **mai viatja per la xarxa**. És el mecanisme natiu d'AD/Samba AD DC:
 1. El client demana un **TGT** (Ticket Granting Ticket) al KDC (el mateix DC) autenticant-se un sol cop.
 2. Amb el TGT, demana **tiquets de servei** (per exemple, per accedir a una compartició) sense tornar a introduir la contrasenya.
 3. Cada servei valida el tiquet sense necessitat de consultar el directori en cada petició.

```
# Obtenir un TGT
kinit jperez@THOS.LOCAL

# Veure els tiquets actuals
klist

# Destruir els tiquets (tancar sessió Kerberos)
kdestroy
```

Aquest mecanisme és el que fa possible el **SSO (Single Sign-On)**: un usuari s'autentica una vegada en iniciar sessió i pot accedir a tots els serveis integrats sense tornar a introduir credencials.

9. Configuració del client per a la integració en el domini

9.1. Client Windows

1. Configurar el DNS del client perquè apunti al DC (imprescindible per a la localització de serveis via SRV).
2. Sistema → Configuració avançada → Nom d'equip → Canviar → Domini i introduir THOS.LOCAL.
3. Autenticar-se amb un compte amb privilegis per unir equips al domini.
4. Reiniciar l'equip.

9.2. Client Linux amb SSSD

SSSD (System Security Services Daemon) és l'estàndard actual als clients Linux per integrar-se amb un directori LDAP/AD, substituint els antics nss_ldap/pam_ldap.

```
sudo apt install sssd sssd-tools realmd adcli krb5-user
↪ samba-common-bin -y

# Descobrir i unir-se al domini automàticament
sudo realm discover thos.local
sudo realm join -U administrator thos.local

# Verificar
sudo realm list
```

Fragment resultant a /etc/sss/sss.conf:

```
[sss]
domains = thos.local
services = nss, pam

[domain/thos.local]
id_provider = ad
access_provider = ad
override_homedir = /home/%u
```

Habilitar la creació automàtica del directori personal en el primer inici de sessió:

```
sudo pam-auth-update --enable mkhomedir
sudo systemctl restart sssd
```

Prova d'integració:

```
id jperez@thos.local
getent passwd jperez@thos.local
su - jperez@thos.local
```

10. Eines gràfiques i ordres per a l'administració

10.1. Ordres (Samba AD DC)

Ordre	Ús
samba-tool user create/list/delete	Gestió d'usuaris
samba-tool group create/addmembers	Gestió de grups
samba-tool computer list	Gestió d'equips units al domini
samba-tool ou create/list	Gestió d'unitats organitzatives
samba-tool domain level show	Nivell funcional del domini
samba-tool drs showrepl	Estat de la replicació entre DC
ldapsearch / ldapmodify	Consulta i modificació LDAP de baix nivell
kinit / klist / kdestroy	Gestió de tiquets Kerberos

Exemple: crear un usuari i afegir-lo a un grup

```
samba-tool user create jperez --given-name=Joan --surname=Pérez \
--userou="OU=Professorat" --mail-address=jperez@thos.local

samba-tool group addmembers "Professorat" jperez
```

10.2. Eines gràfiques

- **RSAT (Remote Server Administration Tools):** eines de Microsoft (*Usuaris i equips d'Active Directory, DNS, GPMC*) que es poden fer servir des d'un client Windows contra un DC Samba, ja que parlen el mateix protocol.
- **Apache Directory Studio:** client LDAP gràfic multiplataforma, útil per inspeccionar l'arbre DIT, l'esquema i executar cerques amb filtres visualment.
- **LDAP Account Manager (LAM):** interfície web per a la gestió d'usuaris i grups en OpenLDAP (i, amb el mòdul corresponent, també en Samba AD DC).

NOTA

És habitual gestionar el dia a dia amb eines gràfiques (RSAT, LAM) i reservar la línia d'ordres (samba-tool, ldapsearch) per a tasques automatitzables (scripts d'alta massiva d'usuaris a principi de curs, per exemple) i per al diagnòstic de problemes.

11. Documentació de l'estructura i la implantació

Documentar el directori és tan important com implantar-lo correctament: sense documentació, qualsevol intervenció futura (pròpia o d'un altre tècnic) és arriscada.

Una documentació completa hauria d'incloure:

1. **Dades bàsiques del domini:** nom NetBIOS, FQDN del realm, nivell funcional, DC existents i el seu rol.
2. **Diagrama de xarxa i topologia de DC,** incloent-hi adreçament IP i ubicació dels rols FSMO (si escau).

3. **Estructura d'OU**, amb la justificació de cada nivell (a quines polítiques respon).
4. **Política de contrasenyes i seguretat** aplicada.
5. **Esquema d'objectes**: convencions de nomenclatura d'usuaris i grups, atributs personalitzats afegits.
6. **Serveis integrats** amb el directori i com hi estan connectats (DNS, fitxers, VPN...).
7. **Procediments de recuperació**: com restaurar un DC, com funciona la replicació, còpies de seguretat del directori (samba-tool domain backup).

Versions d'aquest document

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

[Domini Públic \(CC0\)](#)