Samba AD-DC

Índex

1. Què és Active Directory? 1
1.1. Per què Samba AD-DC? . . . 1

2. Conceptes previs 2
2.1. Protocols implicats . . . 2
2.2. Terminologia . . . 2
2.3. Arquitectura del sistema . . . 3

3. Requisits del sistema 3
3.1. Maquinari mínim recomanat . . . 3
3.2. Programari . . . 4
3.3. Informació del domini (exemple d'aquest document) . . . 4

4. Preparació del servidor 4
4.1. Configuració de la IP estàtica . . . 4
4.2. Configuració del nom d'amfitrió (hostname) . . . 5
4.3. Sincronització horària . . . 6

5. Instal·lació de Samba 7
5.1. Actualitza el sistema . . . 7
5.2. Instal·la els paquets necessaris . . . 7
5.3. Atura i desactiva els serveis per defecte . . . 8
5.4. Activa `samba-ad-dc` . . . 8

6. Aprovisionament del domini 8
6.1. Fes còpia de seguretat de la configuració existent . . . 9
6.2. Executa l'aprovisionament . . . 9
6.3. Desactiva el resolver de systemd (per conflicte de ports DNS) . . . 10
6.4. Copia la configuració de Kerberos . . . 11

7. Configuració del servei 11
7.1. Revisa el fitxer smb.conf generat . . . 11
7.3. Verifica ports en escolta . . . 12

8. Verificació del domini 13
8.1. Verifica el nivell del domini . . . 13
8.2. Verifica DNS . . . 13
8.3. Verifica Kerberos . . . 14
8.4. Verifica LDAP . . . 15
8.5. Verifica SMB . . . 15

9. Gestió d'usuaris i grups 16
9.1. Ordres bàsiques de `samba-tool` . . . 16
Usuaris . . . 16
Grups . . . 17
Unitats Organitzatives (OU) . . . 17
9.2. Exemple: Creació d'estructura departamental . . . 17
9.3. Gestió via RSAT (des de Windows) . . . 18

10. Unió de clients Windows al domini **19**
10.1. Prerequisits del client Windows . . . 19
10.2. Unió al domini (GUI) . . . 20
10.3. Unió al domini (PowerShell) . . . 22
10.4 Verificació . . . 22

11. Unió de clients Linux al domini **22**
11.1. Configuracions prèvies . . . 22
11.2. Sincronitza l'hora . . . 23
11.3. Instal·la els paquets necessaris . . . 24
11.4. Uneix l'equip al domini . . . 24
11.5. Verifica l'inici de sessió . . . 25
11.6. Configura PAM . . . 25

12. Comparticions de xarxa **26**
12.1. Afegeix comparticions a smb.conf . . . 26
12.2. Crea directoris i assigna permisos . . . 26
12.3. Accedeix a les comparticions des de clients . . . 27

13. Directives de grup (GPO) **27**
13.1. Ordres bàsiques de GPO amb samba-tool . . . 27
13.2. Exemple: Política de contrasenyes del domini . . . 28

14. Resolució de problemes **28**
14.1. Ordres de diagnosi . . . 28
14.2. Problemes habituals . . . 28
14.3. Reinici net de l'aprovisionament . . . 29

15. Referència d'ordres **29**
Gestió del domini . . . 29
Gestió d'usuaris . . . 29
Gestió de grups . . . 30
Gestió DNS . . . 30
Kerberos . . . 30
Winbind . . . 30

Annex A: Script de creació massiva d'usuaris **31**

Annex B: Tallafocs (UFW) **31**

Annex C: Seguretat recomanada **32**

16. Documentació i recursos **33**
Documentació oficial . . . 33
Pàgines de manual (`man`) . . . 33
Recursos addicionals . . . 33
Eines de gestió recomanades . . . 34

Cicle formatiu: Sistemes Microinformàtics i Xarxes (SMX)

Mòdul: 0224 --- Sistemes operatius en xarxa

Sistema operatiu: Ubuntu Server 26.04 LTS

Figura 1: Samba logo

Samba és una implementació de codi obert del protocol **SMB/CIFS** que permet la interoperabilitat entre sistemes Linux/Unix i Windows. Des de la versió **4.0**, Samba incorpora la funcionalitat de **Active Directory Domain Controller (AD-DC)**, que permet desplegar un controlador de domini plenament compatible amb l'ecosistema Microsoft Active Directory.

1. Què és Active Directory?

Active Directory (AD) és un servei de directori desenvolupat per Microsoft que proporciona:

- **Autenticació centralitzada** mitjançant Kerberos i NTLM.
- **Autorització** basada en polítiques i grups.
- **Directori LDAP** per emmagatzemar informació d'usuaris, grups i equips.
- **DNS integrat** per a la resolució de noms del domini.
- **Directives de grup (GPO)** per gestionar la configuració dels clients.

1.1. Per què Samba AD-DC?

Característica	Samba AD-DC	Windows Server AD
Llicència	Lliure (GPLv3)	Propietari
Cost	Gratuït	Llicència de pagament
Compatibilitat	Alta (AD-compatible)	Nativa
Rendiment	Excel·lent	Excel·lent
Gestió	Línia d'ordres / RSAT	GUI / PowerShell
Suport GPO complet	Parcial	Complet

NOTA

Samba AD-DC és àmpliament utilitzat en entorns educatius i empresarials que volen aprofitar la infraestructura Active Directory sense el cost de les llicències Microsoft.

2. Conceptes previs

2.1. Protocols implicats

Protocol	Port	Funció
DNS	53 TCP/UDP	Resolució de noms del domini
Kerberos	88 TCP/UDP	Autenticació segura
LDAP	389 TCP/UDP	Accés al directori
LDAPS	636 TCP	LDAP sobre TLS
SMB	445 TCP	Comparticions de fitxers
RPC	135 TCP	Crida a procediments remots
NetBIOS	137-139 TCP/UDP	Compatibilitat llegada
Global Catalog	3268-3269 TCP	Catàleg global AD

2.2. Terminologia

Terme	Definició
Domini	Conjunt d'equips i usuaris administrats centralment
DC (Domain Controller)	Servidor que gestiona el domini
AD-DC	Domain Controller compatible amb Active Directory
FQDN	Nom de domini completament qualificat (ex: `dc1.thos.local`)
NetBIOS	Nom curt del domini (ex: THOS, màx. 15 caràcters)
SID	Identificador de seguretat únic per a cada objecte del domini
GPO	Objecte de directiva de grup per gestionar configuracions
OU	Unitat Organitzativa, contenidor d'objectes AD
SYSVOL	Carpeta compartida on es guarden les GPO i scripts de logon
NETLOGON	Carpeta compartida per als scripts d'inici de sessió

2.3. Arquitectura del sistema

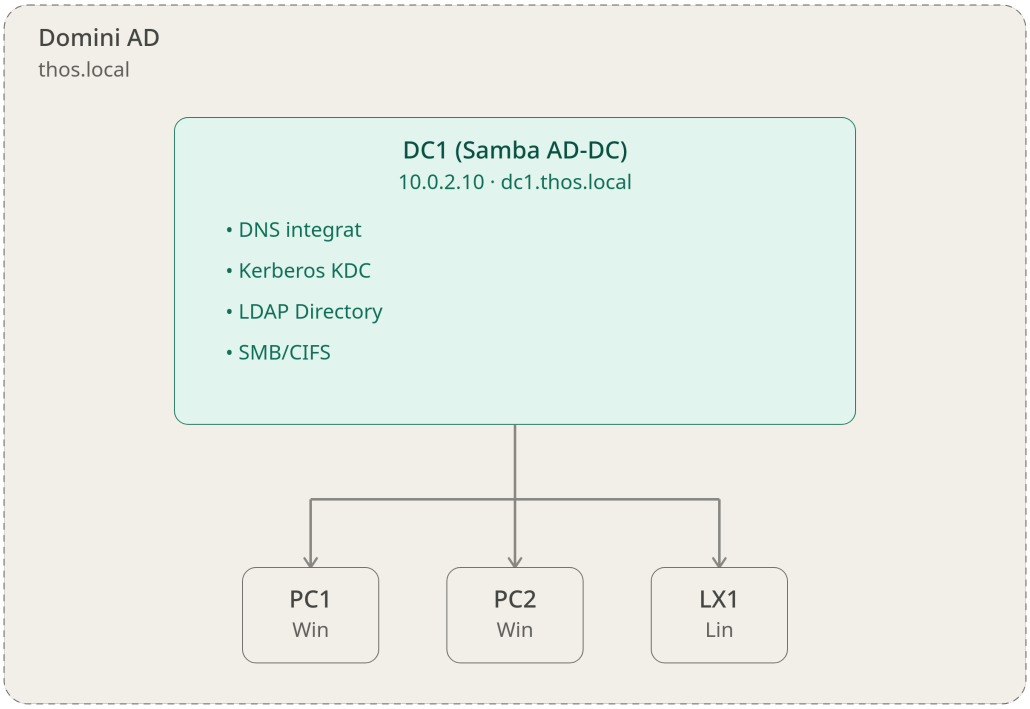

Figura 2: Arquitectura del sistema

3. Requisits del sistema

3.1. Maquinari mínim recomanat

Recurs	Mínim	Recomanat
CPU	1 nucli	2 nuclis
RAM	1 GB	2 GB o més
Disc	20 GB	40 GB o més
Xarxa	1 interfície	1 interfície amb IP estàtica

3.2. Programari

- **Ubuntu Server 26.04 LTS**
- **Samba 4.x** (disponible als dipòsits oficials d'Ubuntu)
- Accés root o sudo

3.3. Informació del domini (exemple d'aquest document)

Paràmetre	Valor d'exemple
Nom del domini (REALM)	`thos.local`
Nom NetBIOS	`THOS`
FQDN del servidor	`dc1.thos.local`
IP del servidor	`10.0.2.10`
Màscara de xarxa	`255.255.255.0`
Password administrador	`P@ssw0rd123` (canviar!)

AVÍS

Substituïu els valors d'exemple pels del vostre entorn real. El domini `.local` pot causar conflictes amb mDNS (Multicast DNS); en producció es recomana usar un subdomini real com `ad.empresa.com`.

4. Preparació del servidor

4.1. Configuració de la IP estàtica

Samba AD-DC requereix una adreça IP estàtica. Editeu la configuració de Netplan:

```
sudo nano /etc/netplan/00-installer-config.yaml
```

```
network:
  ethernets:
    enp0s3:
      addresses:
      - 10.0.2.10/24
      match:
        macaddress: 08:00:27:40:ef:70
      nameservers:
        addresses:
        - 127.0.0.1      # El mateix servidor (DNS intern)
        - 8.8.8.8        # DNS extern com a reserva
        search:
        - thos.local
      routes:
      - to: default
        via: 10.0.2.1
      set-name: enp0s3
```

```
  version: 2
```

Aplica la nova configuració:

```
sudo netplan apply
```

4.2. Configuració del nom d'amfitrió (hostname)

Estableix el nom curt:

```
sudo hostnamectl set-hostname dc1
```

Verifica:

```
hostname
```

Edita `/etc/hosts` per afegir l'FQDN:

```
sudo nano /etc/hosts
```

```
127.0.0.1    localhost
10.0.2.10    dc1.thos.local  dc1
```

IMPORTANT

Elimineu o comenteu qualsevol línia `127.0.1.1` que apunti al nom d'amfitrió, ja que pot causar problemes amb Kerberos.

Verifica la resolució:

```
hostname -f
# Ha de retornar: dc1.thos.local

ping -c 2 dc1.thos.local
```

4.3. Sincronització horària

Kerberos requereix que l'hora del servidor i els clients estigui sincronitzada (tolerància màxima de 5 minuts):

Verifica que el servei de temps està actiu.

```
sudo systemctl status chrony
```

Sortida esperada:

```
● chrony.service - chrony, an NTP client/server
     Loaded: loaded (/usr/lib/systemd/system/chrony.service; enabled;
↪  preset: enabled)
     Active: active (running) since Thu 2026-06-25 07:19:13 UTC; 7min
↪  ago
 Invocation: b597f541b0ce4c128f09e004d99ba093
       Docs: man:chronyd(8)
             man:chronyc(1)
             man:chrony.conf(5)
   Main PID: 1264 (chronyd-starter)
      Tasks: 3 (limit: 1718)
     Memory: 6.7M (peak: 7.2M)
        CPU: 99ms
     CGroup: /system.slice/chrony.service
             ├─1264 /bin/sh
↪  /usr/lib/systemd/scripts/chronyd-starter.sh -n -F 1
             ├─1352 /usr/sbin/chronyd -n -F 1
             └─1367 /usr/sbin/chronyd -n -F 1
```

Estableix el fus horari:

```
sudo timedatectl set-timezone Europe/Madrid
```

Verifica:

```
timedatectl
```

Sortida esperada:

```
               Local time: dj. 2026-06-23 09:31:07 CEST
           Universal time: dj. 2026-06-23 07:31:07 UTC
                 RTC time: dj. 2026-06-23 07:31:07
                Time zone: Europe/Madrid (CEST, +0200)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

Edita chrony per permetre la sincronització amb les màquines de la xarxa local:

```
sudo nano /etc/chrony/chrony.conf
```

Afegeix aquestes línies al final

```
allow 10.0.2.0/24
local stratum 10
```

Reinicia el dimoni

```
sudo systemctl restart chrony
```

5. Instal·lació de Samba

5.1. Actualitza el sistema

Actualitza la llista de paquets

```
sudo apt update
```

Actualita els paquets

```
sudo apt upgrade
```

5.2. Instal·la els paquets necessaris

```
sudo apt install samba-ad-dc samba-ad-provision krb5-config \
    krb5-user winbind libpam-winbind libnss-winbind \
    bind9-dnsutils libpam-krb5 smbclient ldb-tools \
    net-tools dnsutils attr
```

Durant la instal·lació, el sistema demanarà el **realm de Kerberos**. Respostes:

```
THOS.LOCAL
dc1.thos.local
dc1.thos.local
```

5.3. Atura i desactiva els serveis per defecte

Abans d'aprovisionar el domini, cal aturar els serveis de Samba per defecte:

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

I deshabilitar-los:

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

Prepara el servidor per funcionar com a **Active Directory Domain Controller** amb Samba, desactivant els serveis que no cal en aquest mode. Emmascara (bloqueja) els tres serveis del mode Samba clàssic (servidor de fitxers/impressió):

- `smbd` --- servidor SMB (compartició de fitxers)
- `nmbd` --- resolució de noms NetBIOS
- `winbind` --- integració amb dominis Windows

`mask` és més fort que `disable`: crea un symlink a `/dev/null` de manera que **no es poden iniciar ni manualment ni com a dependència** d'un altre servei. Evita conflictes amb `samba-ad-dc`.

```
sudo systemctl mask smbd nmbd winbind
```

5.4. Activa `samba-ad-dc`

Elimina l'emmascarament de `samba-ad-dc`. Aquest servei ve emmascarant per defecte perquè no s'iniciï accidentalment abans de fer la provisió del domini.

```
sudo systemctl unmask samba-ad-dc
```

Activa `samba-ad-dc` perquè s'iniciï automàticament en cada arrencada del sistema.

```
sudo systemctl enable samba-ad-dc
```

6. Aprovisionament del domini

L'aprovisionament crea tota l'estructura del domini AD (base de dades LDAP, zona DNS, configuració de Kerberos, SYSVOL…). Podeu consultar tots els paràmetres disponibles a la documentació de `samba-tool domain provision`.

6.1. Fes còpia de seguretat de la configuració existent

Desa la configuració de Samba per defecte:

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

Desa la configuració de Kerberos per defecte:

```
sudo mv /etc/krb5.conf /etc/krb5.conf.bak
```

6.2. Executa l'aprovisionament

AVÍS

Si el servidor té més d'una interfície de xarxa: `sudo samba-tool domain provision --use-rfc2307 --host-ip=<IP_CORRECTA> --interactive`

```
sudo samba-tool domain provision --use-rfc2307 --interactive
```

Respostes:

```
THOS.LOCAL
THOS
dc
SAMBA_INTERNAL
8.8.8.8
P@ssw0rd123
P@ssw0rd123
```

Significat de les opcions:

Opció	Descripció
`--use-rfc2307`	Afegeix atributs POSIX l'esquema (RFC 2307: UID, GID, shell…) per a clients Linux
Realm	Nom complet del domini Kerberos (en majúscules)
Domain	Nom NetBIOS del domini (màx. 15 caràcters, majúscules)
Server Role	Configura el servidor com a controlador de domini
DNS backend	Usa el DNS intern de Samba (opció recomanada)
DNS forwarder IP address	Aquesta configuració només està disponible quan s'utilitza el backend DNS SAMBA_INTERNAL. El servidor DNS intern només pot resoldre les zones DNS de l'Active Directory (AD). Per habilitar consultes recursives d'altres zones, definiu el paràmetre `dns forwarder` del fitxer `smb.conf` a una o més adreces IP de servidors DNS que admetin la resolució recursiva.
Administrator password	Contrasenya de l'administrador del domini

La sortida esperada és similar a:

```
Realm [THOS.LOCAL]:
Domain [THOS]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
 ↪  [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding)
 ↪  [127.0.0.53]:  8.8.8.8
Administrator password:
Retype password:
...
Setting up sam.ldb partitions and settings: done
Setting up sam.ldb rootDSE: done
Pre-loading the Samba 4 and AD schema: done
A Kerberos configuration suitable for Samba AD has been generated at
 ↪  /var/lib/samba/private/krb5.conf
Setting up share.ldb: done
Setting up secrets.ldb: done
Setting up the registry: done
Setting up the privileges database: done
Setting up idmap db: done
Setting up SAM Database: done
Setting up sam.ldb partitions and settings: done
...
Once the above files are installed, your Samba4 installation will be
 ↪  ready to use.
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        THOS
DNS Domain:            thos.local
DOMAIN SID:            S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX
```

6.3. Desactiva el resolver de systemd (per conflicte de ports DNS)

Samba necessita el port 53. Cal desactivar `systemd-resolved`:

Atura i desactiva systemd-resolved:

```
sudo systemctl stop systemd-resolved
sudo systemctl disable systemd-resolved
```

Elimina l'enllaç simbòlic:

```
sudo rm /etc/resolv.conf
```

Crea un resolv.conf nou que apunti al servidor local:

```
sudo bash -c 'cat > /etc/resolv.conf << EOF
nameserver 127.0.0.1
search thos.local
EOF'
```

6.4. Copia la configuració de Kerberos

```
sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

7. Configuració del servei

7.1. Revisa el fitxer smb.conf generat

L'aprovisionament ha creat `/etc/samba/smb.conf`. Reviseu-lo:

```
cat /etc/samba/smb.conf
```

El contingut típic és:

```
# Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = DC1
    realm = THOS.LOCAL
    server role = active directory domain controller
    workgroup = THOS
    idmap_ldb:use rfc2307 = yes

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/thos.local/scripts
    read only = No
```

Si tens més d'una interfície de xarxa edita el fitxer `/etc/samba/smb.conf`

```
sudo nano /etc/samba/smb.conf
```

Afegeix a l'apartat **`[global]`** aquestes línies:

```
    interfaces = lo enp0s3      # enp0s3 és el nom de la interfície de
↪   xarxa
    bind interfaces only = yes
```

Inicia el servei

```
sudo systemctl start samba-ad-dc
```

Verifica l'estat

```
sudo systemctl status samba-ad-dc
```

La sortida ha de mostrar `active (running)`.

```
● samba-ad-dc.service - Samba AD Daemon
     Loaded: loaded (/usr/lib/systemd/system/samba-ad-dc.service;
 ↪  enabled; preset: enabled)
     Active: active (running) since Wed 2026-06-24 08:24:42 UTC; 1min
 ↪  2s ago
 Invocation: 6f425f30164442ca989aafcc64780137
       Docs: man:samba(8)
             man:samba(7)
             man:smb.conf(5)
    Process: 4489 ExecCondition=/usr/share/samba/is-configured samba
 ↪  (code=exited, status=0/SUCCESS)
   Main PID: 4492 (samba)
     Status: "samba: ready to serve connections..."
      Tasks: 61 (limit: 1718)
     Memory: 189.6M (peak: 243.8M)
        CPU: 2.729s
     CGroup: /system.slice/samba-ad-dc.service
             ├─4492 "samba: root process"
             ├─4493 "samba: tfork waiter process(4494)"
             ├─4494 "samba: task[s3fs] pre-fork master"
             ├─4495 "samba: tfork waiter process(4497)"
             ├─4496 "samba: tfork waiter process(4498)"
             ├─4497 "samba: task[rpc] pre-fork master"
             ├─4498 /usr/sbin/smbd -D "--option=server role
 ↪  check:inhibit=yes" --foreground
             ├─4499 "samba: tfork waiter process(4500)"
```

7.3. Verifica ports en escolta

```
sudo netstat -tulnp | grep samba
```

S'hauria de veure els ports 53, 88, 135, 389, 445, 464, 636, 3268, 3269 en escolta.

```
tcp        0      0 0.0.0.0:3268            0.0.0.0:*
 ↪  LISTEN      4506/samba: task[ld
tcp        0      0 0.0.0.0:3269            0.0.0.0:*
 ↪  LISTEN      4506/samba: task[ld
tcp        0      0 0.0.0.0:135             0.0.0.0:*
 ↪  LISTEN      4504/samba: task[rp
tcp        0      0 0.0.0.0:53              0.0.0.0:*
 ↪  LISTEN      4541/samba: task[dn
tcp        0      0 0.0.0.0:49152           0.0.0.0:*
 ↪  LISTEN      4497/samba: task[rp
```

```
tcp        0      0 0.0.0.0:49153           0.0.0.0:*
 ↪  LISTEN      4504/samba: task[rp
tcp        0      0 0.0.0.0:49154           0.0.0.0:*
 ↪  LISTEN      4504/samba: task[rp
tcp        0      0 0.0.0.0:88              0.0.0.0:*
 ↪  LISTEN      4514/samba: task[kd
tcp        0      0 0.0.0.0:389             0.0.0.0:*
 ↪  LISTEN      4506/samba: task[ld
tcp        0      0 0.0.0.0:464             0.0.0.0:*
 ↪  LISTEN      4514/samba: task[kd
tcp        0      0 0.0.0.0:636             0.0.0.0:*
 ↪  LISTEN      4506/samba: task[ld
tcp6       0      0 :::3268                 :::*
 ↪  LISTEN      4506/samba: task[ld
tcp6       0      0 :::3269                 :::*
 ↪  LISTEN      4506/samba: task[ld
...
```

8. Verificació del domini

8.1. Verifica el nivell del domini

```
sudo samba-tool domain level show
```

Sortida esperada:

```
Domain and forest function level for domain 'DC=thos,DC=local'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

8.2. Verifica DNS

Pregunta al servidor DNS de `127.0.0.1` quina IP té `dc1.thos.local`:

```
host -t A dc1.thos.local 127.0.0.1
```

Sortida esperada:

```
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

dc1.thos.local has address 10.0.2.10
```

Pregunta si el servei Kerberos del domini `thos.local` està al servidor `dc1.thos.local`:

```
host -t SRV _kerberos._tcp.thos.local 127.0.0.1
```

Sortida esperada:

```
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

_kerberos._tcp.thos.local has SRV record 0 100 88 dc1.thos.local.
```

Pregunta si el servei LDAP del domini `thos.local` està al servidor `dc1.thos.local`:

```
host -t SRV _ldap._tcp.thos.local 127.0.0.1
```

Sortida esperada:

```
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

_ldap._tcp.thos.local has SRV record 0 100 389 dc1.thos.local.
```

8.3. Verifica Kerberos

Obté un tiquet Kerberos per a l'administrador

```
kinit administrator
```

Sortida esperada:

```
Password for administrator@THOS.LOCAL:
Warning: Your password will expire in 41 days on dimecres, 5 d'agost
 ↪  de 2026, 08:04:06
```

Verifica el tiquet:

```
klist
```

Sortida esperada:

```
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@THOS.LOCAL

Valid starting    Expires           Service principal
```

```
24/6/26 08:32:45  24/6/26 18:32:45  krbtgt/THOS.LOCAL@THOS.LOCAL
    renew until 25/6/26 08:32:38
```

8.4. Verifica LDAP

Llista el contingut del directori LDAP

```
sudo ldbsearch -H /var/lib/samba/private/sam.ldb \
    -b "DC=thos,DC=local" "(objectClass=domain)" dn
```

Sortida esperada:

```
# record 1
dn: DC=thos,DC=local

# Referral
ref: ldap://thos.local/CN=Configuration,DC=thos,DC=local

# Referral
ref: ldap://thos.local/DC=DomainDnsZones,DC=thos,DC=local

# Referral
ref: ldap://thos.local/DC=ForestDnsZones,DC=thos,DC=local

# returned 4 records
# 1 entries
# 3 referrals
```

8.5. Verifica SMB

Llista les comparticions disponibles

```
smbclient -L localhost -U%
```

Sortida esperada:

```
    Sharename       Type      Comment
    ---------       ----      -------
    sysvol          Disk
    netlogon        Disk
    IPC$            IPC       IPC Service (Samba
 ↪  4.23.6-Ubuntu-4.23.6+dfsg-1ubuntu2.1)
SMB1 disabled -- no workgroup available
```

Connecta a SYSVOL

```
smbclient //localhost/sysvol -U administrator%'P@ssw0rd123'
```

Sortida esperada:

```
Try "help" to get a list of possible commands.
smb: \> l
  .                                   D        0  Wed Jun 24 08:04:06 2026
  ..                                  D        0  Wed Jun 24 08:04:06 2026
  thos.local                          D        0  Wed Jun 24 08:04:05 2026

        11758760 blocks of size 1024. 5895228 blocks available
smb: \> q
```

9. Gestió d'usuaris i grups

9.1. Ordres bàsiques de `samba-tool`

Usuaris

```
# Crear un usuari
sudo samba-tool user create nom.cognom \
    --given-name="Nom" \
    --surname="Cognom" \
    --mail-address="nom.cognom@thos.local" \
    'P@ssw0rdUsuari'

# Llistar usuaris
sudo samba-tool user list

# Mostrar informació d'un usuari
sudo samba-tool user show nom.cognom

# Canviar la contrasenya d'un usuari
sudo samba-tool user setpassword nom.cognom

# Desactivar un usuari
sudo samba-tool user disable nom.cognom

# Activar un usuari
sudo samba-tool user enable nom.cognom

# Eliminar un usuari
sudo samba-tool user delete nom.cognom
```

Grups

```
# Crear un grup
sudo samba-tool group add "Professors"
sudo samba-tool group add "Alumnes"
sudo samba-tool group add "Administradors TI"

# Afegir un membre a un grup
sudo samba-tool group addmembers "Professors" nom.cognom

# Llistar membres d'un grup
sudo samba-tool group listmembers "Professors"

# Llistar tots els grups
sudo samba-tool group list

# Eliminar un membre d'un grup
sudo samba-tool group removemembers "Professors" nom.cognom
```

Unitats Organitzatives (OU)

```
# Crear OU
sudo samba-tool ou create "OU=Departaments,DC=thos,DC=local"
sudo samba-tool ou create "OU=ASIX,OU=Departaments,DC=thos,DC=local"
sudo samba-tool ou create "OU=SMX,OU=Departaments,DC=thos,DC=local"

# Llistar OU
sudo samba-tool ou list
```

9.2. Exemple: Creació d'estructura departamental

```
# Crear estructura d'OU
sudo samba-tool ou create "OU=Centres,DC=thos,DC=local"
sudo samba-tool ou create "OU=Professors,OU=Centres,DC=thos,DC=local"
sudo samba-tool ou create "OU=Alumnes,OU=Centres,DC=thos,DC=local"
sudo samba-tool ou create "OU=Equips,OU=Centres,DC=thos,DC=local"

# Crear grups
sudo samba-tool group add "GRP_Professors" \
    --groupou="OU=Professors,OU=Centres,DC=thos,DC=local"
sudo samba-tool group add "GRP_ASIX" \
    --groupou="OU=Alumnes,OU=Centres,DC=thos,DC=local"
sudo samba-tool group add "GRP_SMX" \
    --groupou="OU=Alumnes,OU=Centres,DC=thos,DC=local"

# Crear usuaris d'exemple
sudo samba-tool user create prof.lopez 'P@ssw0rd' \
    --given-name="Ramon" \
```

```
    --surname="López" \
    --userou="OU=Professors,OU=Centres,DC=thos,DC=local"

sudo samba-tool user create alu.garcia 'P@ssw0rd' \
    --given-name="Joan" \
    --surname="Garcia" \
    --userou="OU=Alumnes,OU=Centres,DC=thos,DC=local"

# Assignar usuaris als grups
sudo samba-tool group addmembers "GRP_Professors" prof.lopez
sudo samba-tool group addmembers "GRP_ASIX" alu.garcia
```

9.3. Gestió via RSAT (des de Windows)

Des d'un client Windows unit al domini, podeu instal·lar les **Remote Server Administration Tools (RSAT)** per gestionar el domini amb interfície gràfica:

```
# PowerShell (Windows 10/11) - com a Administrador
Add-WindowsCapability -Name
 ↪  "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0" -Online
Add-WindowsCapability -Name
 ↪  "Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0" -Online
Add-WindowsCapability -Name "Rsat.DNS.Tools~~~~0.0.1.0" -Online
```

Un cop instal·lades, accediu a:

- **Usuaris i equips d'Active Directory** (`dsa.msc`)
- **Llocs i serveis d'Active Directory** (`dssite.msc`)
- **DNS** (`dnsmgmt.msc`)
- **Administrador de directives de grup** (`gpmc.msc`)

10. Unió de clients Windows al domini

10.1. Prerequisits del client Windows

Abans d'unir un client Windows al domini:

1. **IP del DNS:** configureu el client perquè usi `10.0.2.10` com a servidor DNS primari.
2. **Connectivitat:** verifiqueu que el client pot fer ping al DC (`ping dc1.thos.local`).
3. **Hora sincronitzada:** assegureu-vos que l'hora del client està sincronitzada amb el servidor. Per fer-ho cal anar a: **Tauler de control** → **Rellotge i regió** → **Data i hora** → **Hora d'Internet**

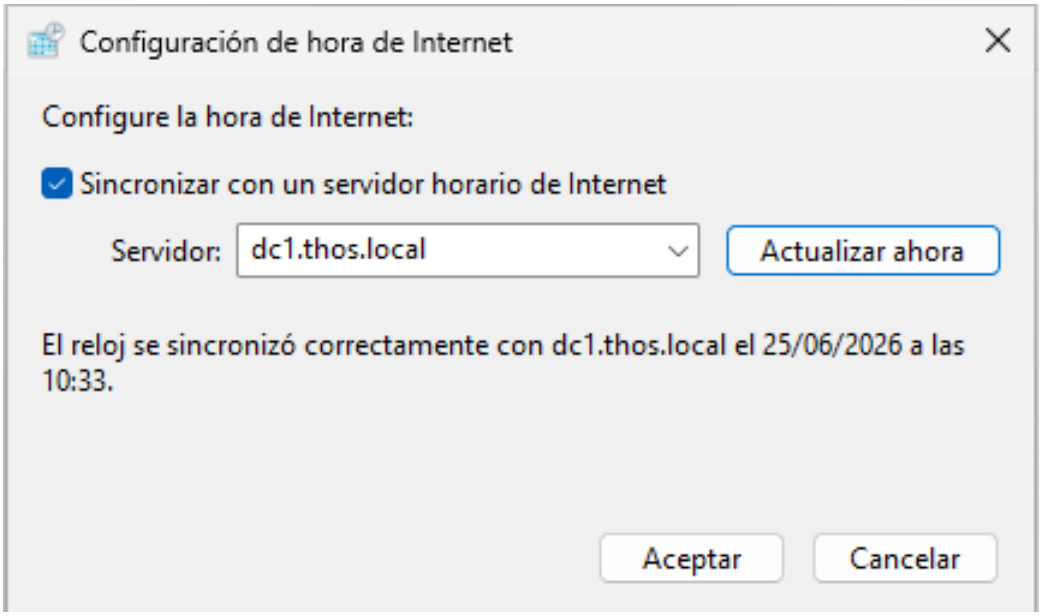

Figura 3: Sincronització de l'hora

10.2. Unió al domini (GUI)

1. Obriu **Propietats del sistema** → **Nom de l'equip** → **Canviar**.
2. Seleccioneu **Domini** i introduïu `thos.local`.
3. Introduïu les credencials de l'administrador del domini.
4. Reinicieu el sistema.

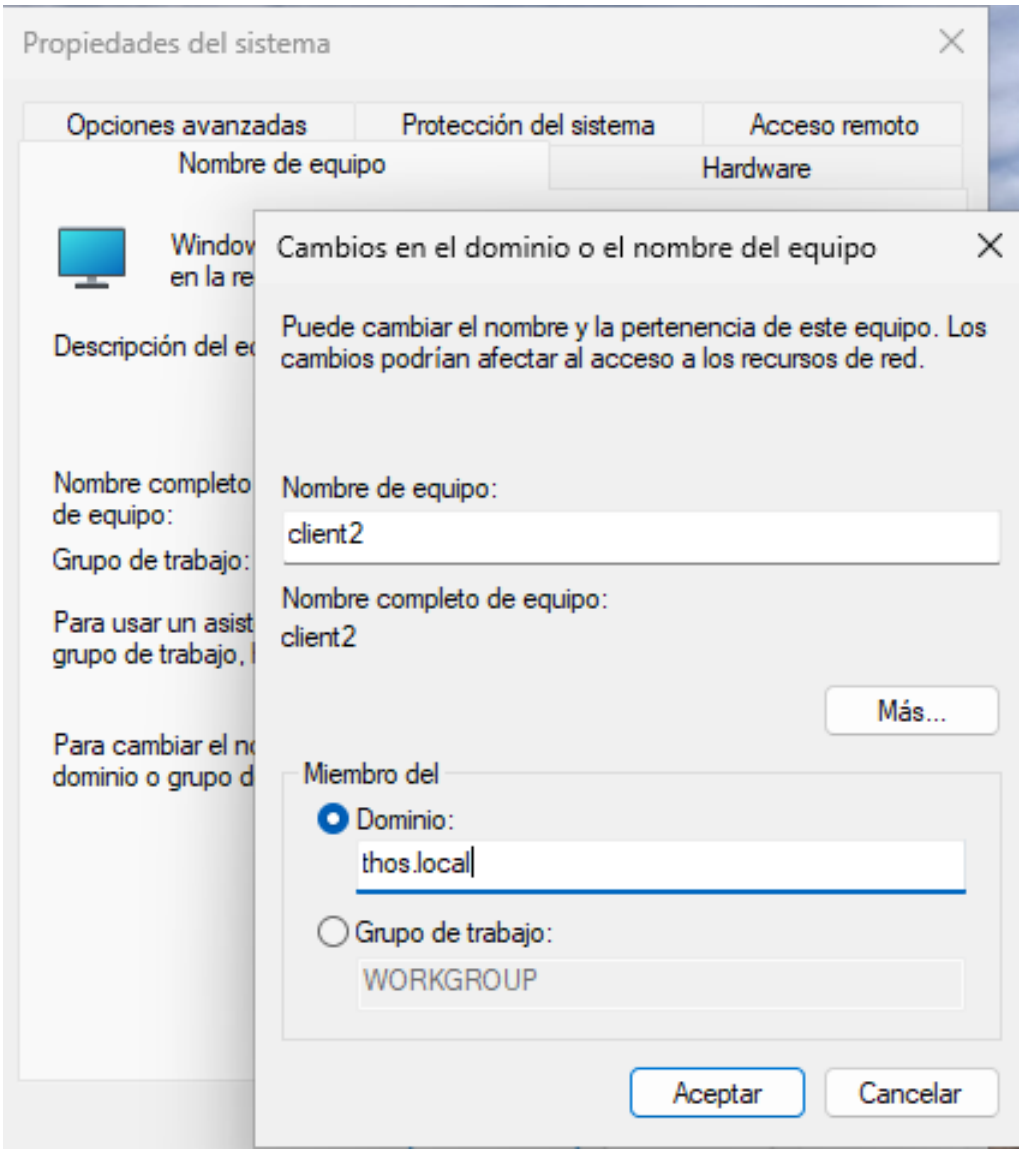

Figura 4: Domini thos.local

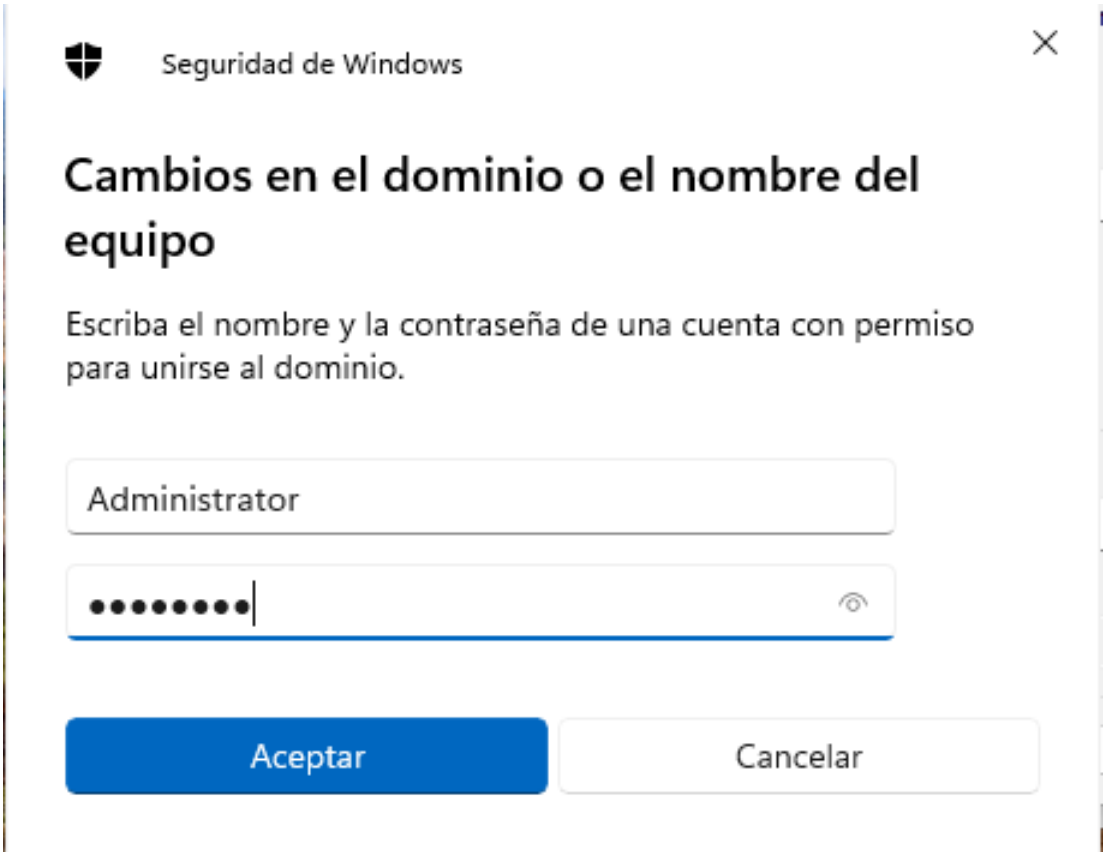

Figura 5: Credencials de l'administrador

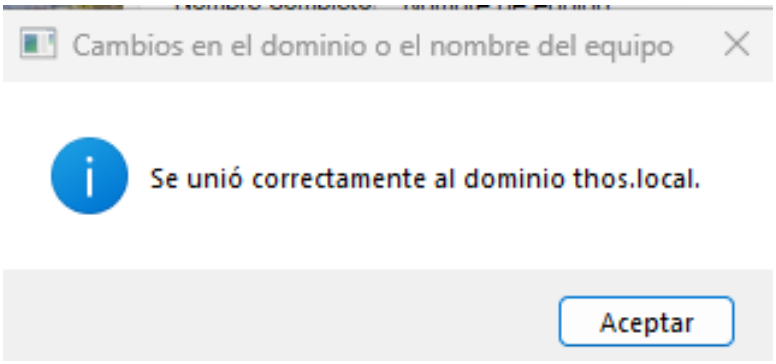

Figura 6: Verificació que s'ha afegit al domini

10.3. Unió al domini (PowerShell)

Executa PowerShell com a Administrador:

```
Add-Computer -DomainName "THOS.LOCAL" -Credential (Get-Credential
 ↪  -UserName "THOS\Administrator") -Restart
```

10.4 Verificació

Des del DC, verifica que l'equip apareix al domini:

```
sudo samba-tool computer list
```

Resposta esperada:

```
DC1$
CLIENT2$
```

11. Unió de clients Linux al domini

11.1. Configuracions prèvies

Modifica el hostname:

```
sudo hostnamectl set-hostname client1
```

Edita el fitxer hosts:

```
sudo nano /etc/hosts
```

```
127.0.1.1 client1.thos.local client1
```

Abans d'unir un client GNU/Linux al domini cal:

1. Configurar el client perquè usi `10.0.2.10` com a servidor DNS primari.
2. Verificar que el client pot fer ping al DC (`ping dc1.thos.local`).

Consulta el nom de la connexió:

```
nmcli con show
```

Sortida:

```
NAME            UUID                                  TYPE      DEVICE
netplan-enp0s3  1eef7e45-3b9d-3043-bee3-fc5925c90273  ethernet  enp0s3
```

```
lo              0d4c85b9-8910-4174-9ef3-667578f0c40d  loopback  lo
```

Configura el domini thos.local explícitament a la connexió `netplan-enp0s3` (canvia aquest nom pel que t'hagi aparegut a tu):

```
sudo nmcli con modify "netplan-enp0s3" ipv4.dns "10.0.2.10"
sudo nmcli con modify "netplan-enp0s3" ipv4.dns-search "thos.local"
sudo nmcli con up "netplan-enp0s3"
```

Verifica la configuració DNS:

```
resolvectl status enp0s3
```

Sortida esperada:

```
Link 2 (enp0s3)
    Current Scopes: DNS
         Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS
 ↪  DNSSEC=no/unsupported
Current DNS Server: 10.0.2.10
       DNS Servers: 10.0.2.10
        DNS Domain: thos.local
     Default Route: yes
```

Verifica que el client pot fer ping:

```
ping dc1.thos.local
```

11.2. Sincronitza l'hora

Esborra la configuració dels servidors d'hora:

```
sudo rm /etc/chrony/sources.d/ubuntu-ntp-pools.sources
```

Crea una nova configuració de servidors d'hora:

```
sudo nano /etc/chrony/sources.d/thos.local.sources
```

```
server dc1.thos.local iburst prefer
```

Reinicia el servei:

```
sudo systemctl restart chrony
```

Sincronitza

```
sudo chronyc makestep
```

Comprova l'estat de la sincronització

```
sudo chronyc sources
```

11.3. Instal·la els paquets necessaris

```
sudo apt install realmd sssd samba-common-bin samba
```

Comprova que l'equip està preparat per unir-se al domini:

```
sudo realm discover thos.local
```

Resposta esperada:

```
thos.local
  type: kerberos
  realm-name: THOS.LOCAL
  domain-name: thos.local
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
```

11.4. Uneix l'equip al domini

```
sudo realm join thos.local -U Administrator
```

Verifica que la màquina està unida al domini:

```
sudo realm list
```

Resposta esperada

```
thos.local
  type: kerberos
  realm-name: THOS.LOCAL
  domain-name: thos.local
  configured: kerberos-member
```

```
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@thos.local
  login-policy: allow-realm-logins
```

11.5. Verifica l'inici de sessió

Inicia sessió amb l'usuari administrador del domini:

```
su THOS\\Administrator
```

Resposta esperada:

```
Contrasenya:
administrator@thos.local@client1:/home/ramon$
```

11.6. Configura PAM

Configura PAM per crear el directori home de l'usuari automàticament:

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

12. Comparticions de xarxa

12.1. Afegeix comparticions a smb.conf

Edita `/etc/samba/smb.conf` per afegir comparticions:

```
sudo nano /etc/samba/smb.conf
```

```
[Global]
    # Configuració existent del domini...

[dades]
    comment = Carpeta de dades compartides
    path = /srv/samba/dades
    browseable = yes
    writable = yes
    valid users = @"THOS\GRP_Professors", @"THOS\GRP_ASIX"
    create mask = 0660
    directory mask = 0770

[professors]
    comment = Recursos per a professors
    path = /srv/samba/professors
    browseable = no
    writable = yes
    valid users = @"THOS\GRP_Professors"
    create mask = 0660
    directory mask = 0770
```

12.2. Crea directoris i assigna permisos

Crea directoris:

```
sudo mkdir -p /srv/samba/dades
sudo mkdir -p /srv/samba/professors
```

Assigna propietari i permisos

```
sudo chown root:"THOS\GRP_Professors" /srv/samba/professors
sudo chmod 2770 /srv/samba/professors

sudo chown root:root /srv/samba/dades
sudo chmod 1777 /srv/samba/dades
```

Reinicia el servei:

```
sudo systemctl restart samba-ad-dc
```

12.3. Accedeix a les comparticions des de clients

Des de Windows:

```
\\dc1\dades
\\dc1\professors
```

Des de Linux:

```
# Muntar una compartició
sudo mount -t cifs //dc1/dades /mnt/dades \
    -o username=nom.cognom,domain=THOS,vers=3.0

# Muntatge permanent a /etc/fstab
//dc1/dades  /mnt/dades  cifs
 ↪  username=nom.cognom,password=P@ss,domain=THOS,vers=3.0  0  0
```

13. Directives de grup (GPO)

Samba admet la gestió de GPO (Group Policy Objects), tot i que amb suport parcial respecte a Windows Server. La forma més còmoda de gestionar GPO és des d'un client Windows amb RSAT.

13.1. Ordres bàsiques de GPO amb samba-tool

```
# Llistar totes les GPO
sudo samba-tool gpo listall

# Crear una nova GPO
sudo samba-tool gpo create "Política de Contrasenyes" \
    -U administrator%'P@ssw0rd123'

# Vincular una GPO a una OU
sudo samba-tool gpo setlink \
    "OU=Alumnes,OU=Centres,DC=thos,DC=local" \
    {GUID_GPO} \
    -U administrator%'P@ssw0rd123'

# Eliminar un vincle
sudo samba-tool gpo dellink \
    "OU=Alumnes,OU=Centres,DC=thos,DC=local" \
    {GUID_GPO} \
    -U administrator%'P@ssw0rd123'
```

13.2. Exemple: Política de contrasenyes del domini

```
# Veure la política de contrasenyes actual
sudo samba-tool domain passwordsettings show

# Modificar la política de contrasenyes
sudo samba-tool domain passwordsettings set \
    --min-pwd-length=8 \
    --min-pwd-age=1 \
    --max-pwd-age=90 \
    --history-length=10 \
    --complexity=on
```

14. Resolució de problemes

14.1. Ordres de diagnosi

```
# Verificar l'estat general del domini
sudo samba-tool domain level show

# Verificar replicació (si hi ha múltiples DC)
sudo samba-tool drs showrepl

# Comprovar els registres DNS del domini
sudo samba-tool dns query dc1 thos.local @ ALL \
    -U administrator%'P@ssw0rd123'

# Veure registres del servei
sudo journalctl -u samba-ad-dc -f
sudo journalctl -u samba-ad-dc --since "1 hour ago"

# Verificar Kerberos
sudo samba-tool user getpassword administrator \
    --attributes=unicodePwd
```

14.2. Problemes habituals

Problema	Causa probable	Solució
El servei no arrenca	Port 53 ocupat per `systemd-resolved`	Desactivar `systemd-resolved`
Error de Kerberos `Clock skew too great`	Diferència horària > 5 min	Sincronitzar l'hora amb NTP
Error DNS `NXDOMAIN`	DNS apunta al servidor incorrecte	Apuntar DNS a `127.0.0.1`
No es pot unir Windows al domini	Tallafoc bloquejant ports	Obrir ports 53, 88, 135, 389, 445
`kinit` falla amb `KDC unreachable`	El servei Samba no corre	`systemctl start samba-ad-dc`
Error `NT_STATUS_NO_LOGON_SERVERS`	smb.conf incorrecte o DC inassolible	Revisar configuració de xarxa

Winbind no resol usuaris	NSS mal configurat	Revisar `/etc/nsswitch.conf`

14.3. Reinici net de l'aprovisionament

Si cal refer l'aprovisionament des de zero:

```
# Atura el servei
sudo systemctl stop samba-ad-dc

# Elimina les dades del domini
sudo rm -rf /var/lib/samba/private/*
sudo rm -rf /var/lib/samba/sysvol/*
sudo rm /etc/samba/smb.conf

# Torna a aprovisionar
sudo samba-tool domain provision ...
```

AVÍS

Això eliminarà tots els usuaris, grups i GPO existents. Feu-ho només en entorns de proves.

15. Referència d'ordres

Gestió del domini

Ordre	Descripció
`samba-tool domain provision`	Provisionar un nou domini
`samba-tool domain level show`	Mostrar el nivell funcional del domini
`samba-tool domain passwordsettings show`	Veure la política de contrasenyes
`samba-tool domain passwordsettings set`	Modificar la política de contrasenyes
`samba-tool drs showrepl`	Mostrar l'estat de replicació

Gestió d'usuaris

Ordre	Descripció
`samba-tool user create <nom> <pass>`	Crear un usuari
`samba-tool user list`	Llistar tots els usuaris
`samba-tool user show <nom>`	Mostrar informació d'un usuari
`samba-tool user setpassword <nom>`	Canviar la contrasenya
`samba-tool user disable <nom>`	Desactivar un usuari
`samba-tool user enable <nom>`	Activar un usuari
`samba-tool user delete <nom>`	Eliminar un usuari

Gestió de grups

Ordre	Descripció
`samba-tool group add <nom>`	Crear un grup
`samba-tool group list`	Llistar tots els grups
`samba-tool group listmembers <nom>`	Llistar membres d'un grup
`samba-tool group addmembers <grup> <usuari>`	Afegir membre al grup
`samba-tool group removemembers <grup> <usuari>`	Eliminar membre del grup
`samba-tool group delete <nom>`	Eliminar un grup

Gestió DNS

Ordre	Descripció
`samba-tool dns query <dc> <zona> @ ALL`	Consultar els registres d'una zona
`samba-tool dns query <dc> <zona> <host> <tipus>`	Registres d'un host concret
`samba-tool dns add <dc> <zona> <host> A <IP>`	Afegir registre A
`samba-tool dns delete <dc> <zona> <host> A <IP>`	Eliminar registre A
`samba-tool dns zonelist <dc>`	Llistar zones DNS
`samba-tool dns query <dc> _tcp SRV`	Registres SRV (Kerberos, LDAP…)

Kerberos

Ordre	Descripció
`kinit <usuari>@DOMINI`	Obtenir un tiquet Kerberos
`klist`	Llistar tiquets actius
`kdestroy`	Eliminar tots els tiquets

Winbind

Ordre	Descripció
`wbinfo -u`	Llistar usuaris del domini
`wbinfo -g`	Llistar grups del domini
`wbinfo -a <usuari>%<pass>`	Autenticar un usuari
`wbinfo --ping-dc`	Verificar connexió amb el DC
`net ads info`	Informació sobre el domini AD
`net ads join -k`	Unir un client al domini

Annex A: Script de creació massiva d'usuaris

```
#!/bin/bash
# create_users.sh - Creació massiva d'usuaris al domini Samba AD-DC
# Ús: ./create_users.sh usuaris.csv
# Format CSV: nom,cognom,username,ou,grup

DOMAIN="thos.local"
DEFAULT_PASS="Canvia@2026"
DC_BASE="DC=thos,DC=local"

while IFS=',' read -r nom cognom username ou grup; do
    echo "Creant usuari: $username ($nom $cognom)"

    sudo samba-tool user create "$username" "$DEFAULT_PASS" \
        --given-name="$nom" \
        --surname="$cognom" \
        --mail-address="${username}@${DOMAIN}" \
        --userou="OU=${ou},${DC_BASE}" \
        --must-change-at-next-login

    sudo samba-tool group addmembers "$grup" "$username"

done < "$1"

echo "Creació d'usuaris completada."
```

Fitxer CSV d'exemple (`usuaris.csv`):

```
Joan,Garcia,joan.garcia,Alumnes,GRP_ASIX
Anna,Pérez,anna.perez,Alumnes,GRP_SMX
Pere,Martí,pere.marti,Professors,GRP_Professors
```

Annex B: Tallafocs (UFW)

Si teniu UFW activat al servidor DC, obriu els ports necessaris:

```
sudo ufw allow 53/tcp comment "DNS"
sudo ufw allow 53/udp comment "DNS"
sudo ufw allow 88/tcp comment "Kerberos"
sudo ufw allow 88/udp comment "Kerberos"
sudo ufw allow 135/tcp comment "RPC"
sudo ufw allow 137/udp comment "NetBIOS"
sudo ufw allow 138/udp comment "NetBIOS"
sudo ufw allow 139/tcp comment "NetBIOS"
sudo ufw allow 389/tcp comment "LDAP"
sudo ufw allow 389/udp comment "LDAP"
sudo ufw allow 445/tcp comment "SMB"
sudo ufw allow 464/tcp comment "Kerberos Password"
```

```
sudo ufw allow 464/udp comment "Kerberos Password"
sudo ufw allow 636/tcp comment "LDAPS"
sudo ufw allow 3268/tcp comment "Global Catalog"
sudo ufw allow 3269/tcp comment "Global Catalog SSL"
sudo ufw allow 49152:65535/tcp comment "RPC Dynamic Ports"

sudo ufw reload
sudo ufw status numbered
```

Annex C: Seguretat recomanada

1. **Contrasenyes fortes:** Estabiu polítiques de contrasenya amb longitud mínima de 10 caràcters, complexitat obligatòria i rotació periòdica.
2. **LDAPS (LDAP sobre TLS):** Configureu certificats TLS per xifrar les comunicacions LDAP.
3. **Còpies de seguretat regulars:** Feu còpies de `/var/lib/samba/private/` i `/var/lib/samba/sysvol/`.
4. **Monitoratge:** Reviseu regularment els registres d'autenticació a `/var/log/samba/`.
5. **Principi de mínim privilegi:** No useu el compte `administrator` per a tasques diàries. Creeu comptes d'administrador específics.
6. **Actualitzacions:** Manteniu Samba actualitzat per rebre pedaços de seguretat.

```
# Còpia de seguretat del domini
sudo tar czf /backup/samba-$(date +%Y%m%d).tar.gz \
    /var/lib/samba/private/ \
    /var/lib/samba/sysvol/ \
    /etc/samba/smb.conf \
    /etc/krb5.conf
```

16. Documentació i recursos

Documentació oficial

Recurs	Descripció
Wiki de Samba	Documentació oficial i completa de Samba
Samba AD-DC: Setup Guide	Guia oficial de configuració de Samba com AD-DC
Samba: Joining clients to AD	Unió de clients Linux al domini
Samba: DNS Administration	Administració del DNS integrat de Samba
Samba: Group Policy	Gestió de directives de grup
Samba: Winbind	Integració de clients Linux amb AD
Samba: Troubleshooting AD DC	Resolució de problemes del DC
Ubuntu Server Guide	Documentació oficial d'Ubuntu Server
Netplan Reference	Referència de la sintaxi YAML de Netplan
MIT Kerberos Documentation	Documentació completa de Kerberos

Pàgines de manual (`man`)

```
man samba-tool        # Referència completa de samba-tool
man smb.conf          # Opcions de configuració de Samba
man wbinfo            # Eines de consulta Winbind
man kinit             # Obtenció de tickets Kerberos
man net               # Eina de xarxa de Samba
man smbclient         # Client SMB/CIFS
man ldbsearch         # Consultes LDAP a les bases de dades de Samba
man realm             # Gestió de dominis amb realmd
```

Recursos addicionals

Recurs	Descripció
Samba Release Notes	Notes de versions de Samba
RFC 2307	Esquema LDAP per a atributs POSIX Unix
RFC 4120	Protocol Kerberos V5
MS-ADTS (Microsoft)	Especificació tècnica de Active Directory
realmd Documentation	Documentació de realmd
SSSD Documentation	Documentació de SSSD
UFW (Ubuntu Firewall)	Configuració del tallafocs UFW

Eines de gestió recomanades

Eina	Plataforma	Descripció
RSAT	Windows	Gestió gràfica d'AD (usuaris, GPO, DNS)
LAM (LDAP Account Manager)	Web	Interfície web per gestionar comptes LDAP/AD
Apache Directory Studio	Multiplataforma	Client LDAP amb interfície gràfica

Versions d'aquest document

- HTML - samba-ad-dc.html
- PDF - samba-ad-dc.pdf
- ODT - samba-ad-dc.odt
- MD - samba-ad-dc.md