

# **Controlador de domini Linux amb Samba**

M04 Sistemes operatius en xarxa – UF4

Álvaro Soto Manzino

04/03/2024

# Índex

Índex.....	2
1. Configuració Linux server.....	3
1.1. Configuració de la xarxa.....	3
1.2. Instal·lació i configuració inicial de DC samba.....	4
1.3. Comprovacions.....	7
2. Configuració d'usuaris i grups en DC Samba.....	9
2.1. Creació d'usuaris.....	9
2.2. Creació de grups.....	10
3. Afegim clients al domini.....	11
3.1. Configuració client Linux.....	11
3.1.1. Configuració de xarxa.....	11
3.1.2. Configuració de domini.....	13
3.2. Configuració client Windows.....	16
3.2.1. Configuració de xarxa.....	16
3.2.2. Configuració de domini.....	17
4. Administració de AD Samba des de Windows.....	22
4.1. Instal·lació RSAT.....	22
4.3 Creació de GPOs.....	26
4.3.1 GPO perfil mòbil.....	27
Webgrafia.....	30

# 1. Configuració Linux server

## 1.1. Configuració de la xarxa

Primer llistem les connexions de xarxa que tenim i ens fixem en la que té com a DEVICE **enp2s0**, necessitarem saber el nom de la connexió per al pas següent.

```
[asoto@fedora ~]$ nmcli connection show
```

NAME	UUID	TYPE	DEVICE
Conexión cableada 1	aa87bab8-a020-3e18-aacc-d90f41db0525	ethernet	enp1s0
Conexión cableada 2	ecc534d0-a76d-38cf-973e-91eec3a37ca0	ethernet	enp2s0
lo	9fbf17e8-8747-4296-9778-9415c5394036	loopback	lo

Amb la següent comanda configurem la IP de la interfície fent servir el nom de la connexió.

```
[asoto@fedora ~]$ nmcli connection modify "Conexión cableada 2" ipv4.addresses 192.168.216.1/24 ipv4.method manual
```

Comprovem que s'ha configurat correctament amb **nmcli device show**.

```
[asoto@fedora ~]$ nmcli device show enp2s0
```

GENERAL.DEVICE:	enp2s0
GENERAL.TYPE:	ethernet
GENERAL.HWADDR:	52:54:00:61:0C:8F
GENERAL.MTU:	1500
GENERAL.STATE:	100 (conectado)
GENERAL.CONNECTION:	Conexión cableada 2
GENERAL.CON-PATH:	/org/freedesktop/NetworkManager/ActiveConnection/19
WIRED-PROPERTIES.CARRIER:	activado
IP4.ADDRESS[1]:	<u>192.168.216.1/24</u>
IP4.GATEWAY:	--
IP4.ROUTE[1]:	dst = 192.168.216.0/24, nh = 0.0.0.0, mt = 101
IP6.ADDRESS[1]:	fe80::7f9c:6302:bb8f:a843/64
IP6.GATEWAY:	--
IP6.ROUTE[1]:	dst = fe80::/64, nh = ::, mt = 1024

Actualitzem els repositoris amb **dnf update** abans d'instal·lar qualsevol paquet.

```
[asoto@fedora ~]$ sudo dnf update
[sudo] contraseña para asoto:
Última comprobación de caducidad de metadatos hecha hace 0:05:43, el jue 29 feb 2024 17:41:16.
Dependencias resueltas.
```

## 1.2. Instal·lació i configuració inicial de DC samba

Instal·lem els paquets necessaris per a crear un DC de samba.

```
[asoto@fedora ~]$ sudo dnf install -y samba samba-dc samba-client krb5-workstation
```

Canviem el nom de la màquina.

```
[asoto@fedora ~]$ sudo hostnamectl set-hostname ad-cyn.asoto.foo
```

```
[asoto@ad-cyn ~]$ hostname  
ad-cyn.asoto.foo
```

Obrim els ports que farà servir samba en el Firewall.

```
[asoto@ad-cyn ~]$ sudo firewall-cmd --permanent --add-service samba-dc  
[sudo] contraseña para asoto:  
success
```

Reiniciem el Firewall.

```
[asoto@ad-cyn ~]$ sudo firewall-cmd --reload  
success
```

Executem la següent comanda per canviar els següents valors booleans de [SELinux](#).

```
[asoto@ad-cyn ~]$ sudo setsebool -P samba_create_home_dirs=on samba_domain_controller=on \  
> samba_enable_home_dirs=on samba_portmapper=on use_samba_home_dirs=on
```

Amb [getsebool](#) comprovem que els valors s'han canviat.

```
[asoto@ad-cyn ~]$ sudo getsebool -a | grep samba | grep " on"  
samba_create_home_dirs --> on  
samba_domain_controller --> on  
samba_enable_home_dirs --> on  
samba_portmapper --> on  
use_samba_home_dirs --> on
```

Ara hem de fer que s'utilitzi el DNS que porta incorporat samba en lloc de **systemd-resolved**.

Primer reanomenem el fitxer **smb.conf**.

```
[asoto@ad-cyn ~]$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.no
```

Creem el directori **/etc/systemd/resolved.conf.d**.

```
[asoto@ad-cyn ~]$ sudo mkdir /etc/systemd/resolved.conf.d
```

Dins del directori que hem creat, creem l'arxiu **custom.conf** i l'editem.

```
[asoto@ad-cyn ~]$ sudo nvim /etc/systemd/resolved.conf.d/custom.conf
```

Afegim les següents línies.

```
[Resolve]
DNSStubListener=no
Domains=asoto.foo
DNS=192.168.216.1
```

Reiniciem el servei **systemd-resolved** i comprovem que funciona correctament.

```
[asoto@ad-cyn ~]$ sudo systemctl restart systemd-resolved
[asoto@ad-cyn ~]$ sudo systemctl status systemd-resolved
[sudo] contraseña para asoto:
● systemd-resolved.service - Network Name Resolution
   Loaded: loaded (/usr/lib/systemd/system/systemd-resolved.service; enabled; preset: enabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Mon 2024-03-04 19:00:48 CET; 5min ago
     Docs: man:systemd-resolved.service(8)
           man:org.freedesktop.resolve1(5)
           https://www.freedesktop.org/wiki/Software/systemd/writing-network-configuration-managers
           https://www.freedesktop.org/wiki/Software/systemd/writing-resolver-clients
  Main PID: 4129 (systemd-resolve)
    Status: "Processing requests..."
     Tasks: 1 (limit: 9475)
    Memory: 4.9M
       CPU: 111ms
    CGroup: /system.slice/systemd-resolved.service
            └─4129 /usr/lib/systemd/systemd-resolved
```

Ara podem promoure el servidor a controlador de domini amb la següent comanda

```
[asoto@ad-cyn ~]$ sudo samba-tool domain provision --server-role=dc --use-rfc2307 \
> --dns-backend=SAMBA_INTERNAL --realm=ASOTO.FOO --domain=ASOTO --adminpass=P@ssw0rd
```

Aquesta comanda genera un nou arxiu **smb.conf**

```
[asoto@ad-cyn ~]$ sudo nvim /etc/samba/smb.conf
# Global parameters
[global]
    dns forwarder = 192.168.216.1
    netbios name = AD-CYN
    realm = ASOTO.FOO
    server role = active directory domain controller
    workgroup = ASOTO
    idmap_ldb:use rfc2307 = yes

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

[netlogon]
    path = /var/lib/samba/sysvol/asoto.foo/scripts
    read only = No
~
```

Aquesta instal·lació genera un nou arxiu **krb5.conf**, el copiem a **/etc/krb5.conf.d/samba-dc**

```
[asoto@ad-cyn ~]$ sudo cp /usr/share/samba/setup/krb5.conf /etc/krb5.conf.d/samba-dc
```

Editem l'arxiu i canviem **\${REALM}** pel nostre nom de domini

```
[libdefaults]
    default_realm = ${REALM}
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
${REALM} = {
    default_domain = ${DNSDOMAIN}
}

[domain_realm]
    ${HOSTNAME} = ${REALM}
```

```
[libdefaults]
    default_realm = ASOTO.FOO
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
ASOTO.FOO = {
    default_domain = ASOTO
}

[domain_realm]
    ad-cyn.asoto.foo = ASOTO.FOO
```

Habilitem i iniciem el servei de samba

```
[asoto@ad-cyn ~]$ sudo systemctl enable samba
[sudo] contraseña para asoto:
Created symlink /etc/systemd/system/multi-user.target.wants/samba.service from /usr/lib/systemd/system/samba.service.
[asoto@ad-cyn ~]$ sudo systemctl start samba
```

### 1.3. Comprovacions

#### XARXA:

Amb la comanda **smbclient** comprovem la connectivitat.

```
[asoto@ad-cyn ~]$ smbclient -L localhost -N
Anonymous login successful

      Sharename      Type      Comment
      -----      -
      sysvol         Disk
      netlogon       Disk
      IPC$           IPC       IPC Service (Samba 4.18.10)
SMB1 disabled -- no workgroup available
```

Veiem que el servei funciona correctament.

Comprovem que podem iniciar sessió amb el compte d'administrador.

```
[asoto@ad-cyn ~]$ smbclient //localhost/netlogon -U Administrator -c 'ls'
Password for [ASOTO\Administrator]:
.                               D           0   Mon Mar   4 19:15:25 2024
..                              D           0   Mon Mar   4 19:15:29 2024

82834432 blocks of size 1024. 75818608 blocks available
```

## DNS:

Comprovem que la resolució de noms funciona correctament.

```
[asoto@ad-cyn ~]$ host -t SRV _ldap._tcp.asoto.foo.
_ldap._tcp.asoto.foo has SRV record 0 100 389 ad-cyn.asoto.foo.
```

```
[asoto@ad-cyn ~]$ host -t SRV _kerberos._udp.asoto.foo.
_kerberos._udp.asoto.foo has SRV record 0 100 88 ad-cyn.asoto.foo.
```

```
[asoto@ad-cyn ~]$ host -t A ad-cyn.asoto.foo
ad-cyn.asoto.foo has address 192.168.120.124
ad-cyn.asoto.foo has address 192.168.216.1
[asoto@ad-cyn ~]$
```

## KERBEROS:

Comprovem que Kerberos funciona correctament.

```
[asoto@ad-cyn ~]$ kinit administrator
Password for administrator@ASOTO.FOO:
```

```
[asoto@ad-cyn ~]$ klist
Ticket cache: KCM:1000
Default principal: administrator@ASOTO.FOO

Valid starting    Expires          Service principal
04/03/24 20:14:46 05/03/24 06:14:46 krbtgt/ASOTO.FOO@ASOTO.FOO
renew until 11/03/24 20:14:43
```

Reiniciem el servidor amb **sudo reboot** i tindrem el controlador de domini funcionant.



## 2. Configuració d'usuaris i grups en DC Samba

### 2.1. Creació d'usuaris

Ara procedirem a crear dos usuaris de samba.

Per crear un usuari, fem servir la comanda **samba-tool user create**, especificant el nom d'usuari i uns quants altres paràmetres.

```
[asoto@ad-cyn ~]$ sudo samba-tool user create alvaro P@ssw0rd \  
> --use-username-as-cn --given-name="Alvaro" --surname="Soto" \  
> --must-change-at-next-login  
[sudo] contraseña para asoto:  
User 'alvaro' added successfully
```

Indiquem el nom d'usuari, la contrasenya i...

**--use-username-as-cn** per a que s'utilitzi el nom d'usuari com a *common name*.

**--given-name** i **--surname** per configurar el nom i cognom de l'usuari.

**--must-change-at-next-login** per forçar a l'usuari a canviar la contrasenya la pròxima vegada que iniciï sessió.

Amb la comanda **pdbedit -L** comprovem que s'ha creat l'usuari.

```
[asoto@ad-cyn ~]$ sudo !!  
sudo pdbedit -L  
[sudo] contraseña para asoto:  
Administrator:4294967295:  
nobody:65534:Kernel Overflow User  
krbtgt:4294967295:  
alvaro:4294967295:Alvaro Soto  
AD-CYN$:4294967295:
```

Creem un segon usuari.

```
[asoto@ad-cyn ~]$ sudo samba-tool user create ainhoa P@ssw0rd \  
> --use-username-as-cn --given-name="Ainhua" --surname="Soto" \  
> --must-change-at-next-login  
[sudo] contraseña para asoto:  
User 'ainhoa' added successfully
```

I comprovem que s'ha afegit correctament.

```
[asoto@ad-cyn ~]$ sudo pdbedit -L
Administrator:4294967295:
ainhoa:4294967295:Ainhwa Soto
nobody:65534:Kernel Overflow User
krbtgt:4294967295:
alvaro:4294967295:Alvaro Soto
AD-CYN$:4294967295:
```

## 2.2. Creació de grups

Creem un grup al qual pertanyeran els usuaris.

```
[asoto@ad-cyn ~]$ sudo samba-tool group add hermanos
Added group hermanos
```

Afegim els dos usuaris al grup amb **group addmembers**

```
[asoto@ad-cyn ~]$ sudo samba-tool group addmembers hermanos alvaro,ainhoa
[sudo] contraseña para asoto:
Added members to group hermanos
```

Comprovem que s'han afegit.

```
[asoto@ad-cyn ~]$ sudo samba-tool group listmembers hermanos
ainhoa
alvaro
```

## 3. Afegim clients al domini

### 3.1. Configuració client Linux

#### 3.1.1. Configuració de xarxa

Primer configurem el client Linux per a que estigui en la mateixa xarxa que el servidor

Entrem a l'arxiu **/etc/network/interfaces** i l'editem

```
local@cliente-v:~$ sudo vim /etc/network/interfaces
```

Configurem les dues interfícies de la següent manera

```
auto enp1s0
iface enp1s0 inet dhcp

auto enp2s0
iface enp2s0 inet static
address 192.168.216.2
netmask 255.255.255.0
gateway 192.168.216.1
```

Per a aplicar els canvis, reiniciem el servei **networking**

```
local@cliente-v:~$ sudo systemctl restart networking
```

```
local@cliente-v:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    link/ether 52:54:00:13:e4:38 brd ff:ff:ff:ff:ff:ff
    inet 192.168.123.233/22 brd 192.168.123.255 scope global dynamic
        valid_lft 2895sec preferred_lft 2895sec
    inet6 fe80::5054:ff:fe13:e438/64 scope link
        valid_lft forever preferred_lft forever
3: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    link/ether 52:54:00:1f:dc:94 brd ff:ff:ff:ff:ff:ff
    inet 192.168.216.2/24 brd 192.168.216.255 scope global enp2s0
        valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe1f:dc94/64 scope link
        valid_lft forever preferred_lft forever
```

Comprovem que hi ha connectivitat

```
local@cliente-v:~$ ping -c 4 192.168.216.1
PING 192.168.216.1 (192.168.216.1) 56(84) bytes of data.
64 bytes from 192.168.216.1: icmp_seq=1 ttl=64 time=0.277 ms
64 bytes from 192.168.216.1: icmp_seq=2 ttl=64 time=0.233 ms
64 bytes from 192.168.216.1: icmp_seq=3 ttl=64 time=0.272 ms
64 bytes from 192.168.216.1: icmp_seq=4 ttl=64 time=0.265 ms

--- 192.168.216.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.233/0.261/0.277/0.017 ms
```

Editam l'arxiu **/etc/resolv.conf** i l'editem per a que faci servir el DNS de Samba

```
local@cliente-v:~$ sudo vim /etc/resolv.conf
```

```
nameserver 192.168.216.1
search asoto.foo
~
```

Comprovem que funciona la resolució de noms

```
local@cliente-v:~$ ping -c 4 ad-cyn
PING ad-cyn.asoto.foo (192.168.216.1) 56(84) bytes of data.
64 bytes from 192.168.216.1 (192.168.216.1): icmp_seq=1 ttl=64 time=0.178 ms
64 bytes from 192.168.216.1 (192.168.216.1): icmp_seq=2 ttl=64 time=0.254 ms
64 bytes from 192.168.216.1 (192.168.216.1): icmp_seq=3 ttl=64 time=0.170 ms
64 bytes from 192.168.216.1: icmp_seq=4 ttl=64 time=0.167 ms

--- ad-cyn.asoto.foo ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3260ms
rtt min/avg/max/mdev = 0.167/0.192/0.254/0.035 ms
```

```
local@cliente-v:~$ ping -c 4 ad-cyn.asoto.foo
PING ad-cyn.asoto.foo (192.168.216.1) 56(84) bytes of data.
64 bytes from 192.168.216.1 (192.168.216.1): icmp_seq=1 ttl=64 time=0.097 ms
64 bytes from 192.168.216.1 (192.168.216.1): icmp_seq=2 ttl=64 time=0.161 ms
64 bytes from 192.168.216.1 (192.168.216.1): icmp_seq=3 ttl=64 time=0.219 ms
64 bytes from 192.168.216.1: icmp_seq=4 ttl=64 time=0.190 ms

--- ad-cyn.asoto.foo ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3504ms
rtt min/avg/max/mdev = 0.097/0.166/0.219/0.045 ms
```

```
local@cliente-v:~$ nslookup asoto.foo
Server:      192.168.216.1
Address:     192.168.216.1#53

Name:   asoto.foo
Address: 192.168.216.1
Name:   asoto.foo
Address: 192.168.120.122
```

### 3.1.2. Configuració de domini

Per a poder iniciar sessió al client amb usuaris de domini, primer hem d'instal·lar els següents paquets. El més important d'aquests és **sssd**, que administra l'autenticació d'usuari.

```
local@cliente-v:~$ sudo apt install sssd-ad sssd-tools realmd adcli
S'està llegint la llista de paquets. Fet
```

Ara procedim a afegir el client al domini amb **realmd**

Primer, ens assegurem que el domini es pot descobrir amb DNS

```
local@cliente-v:~$ sudo realm -v discover asoto.foo
* Resolving: _ldap._tcp.asoto.foo
* Performing LDAP DSE lookup on: 192.168.120.122
* Performing LDAP DSE lookup on: 192.168.216.1
* Successfully discovered: asoto.foo
asoto.foo
  type: kerberos
  realm-name: ASOTO.FOO
  domain-name: asoto.foo
  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
```

Com veiem, realmd pot trobar el domini, així que ens podem unir

```
local@cliente-v:~$ sudo realm join asoto.foo
Contrasenya per Administrator:
```

Ara hem de configurar SSSD. Primer anem a l'arxiu **/etc/sss/sss.conf**

```
[sssd]
domains = asoto.foo
config_file_version = 2
services = nss, pam

[domain/asoto.foo]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = ASOTO.FOO
realmd_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = asoto.foo
use_fully_qualified_names = True
ldap_id_mapping = True
access_provider = ad
```

Veiem que ja hi han configurats varis paràmetres de usuari de domini.

Una de les coses que no ha configurat sssd és la creació de directoris *home* per als usuaris de domini. Per a habilitar-ho, executem la següent comanda per habilitar **pam-mkhomedir**.

```
local@cliente-v:~$ sudo pam-auth-update --enable mkhomedir
```

Amb això ja estem connectats al domini. Ara podem accedir a la informació sobre el domini.

Veiem les carpetes compartides.

```
local@cliente-v:~$ smbclient -L asoto.foo -U Administrator
Password for [WORKGROUP\Administrator]:

      Sharename      Type      Comment
      -----
      sysvol         Disk
      netlogon       Disk
      IPC$           IPC       IPC Service (Samba 4.18.10)
SMB1 disabled -- no workgroup available
```

Veiem informació sobre l'usuari **alvaro**.

```
local@cliente-v:~$ getent passwd alvaro@asoto.foo
alvaro@asoto.foo:*:854201103:854200513:alvaro:/home/alvaro@asoto.foo:/bin/bash
```

Veiem els grups dels quals forma part.

```
local@cliente-v:~$ groups alvaro@asoto.foo
alvaro@asoto.foo : domain users@asoto.foo hermanos@asoto.foo
```



I finalment iniciem sessió amb l'usuari.

```
local@cliente-v:~$ sudo login
cliente-v usuari: alvaro@asoto.foo
Contrasenya:
La contrasenya ha vençut. Canvieu ara la vostra contrasenya.
Contrasenya actual:
Nova contrasenya:
Torneu a escriure la nova contrasenya:
Linux cliente-v 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

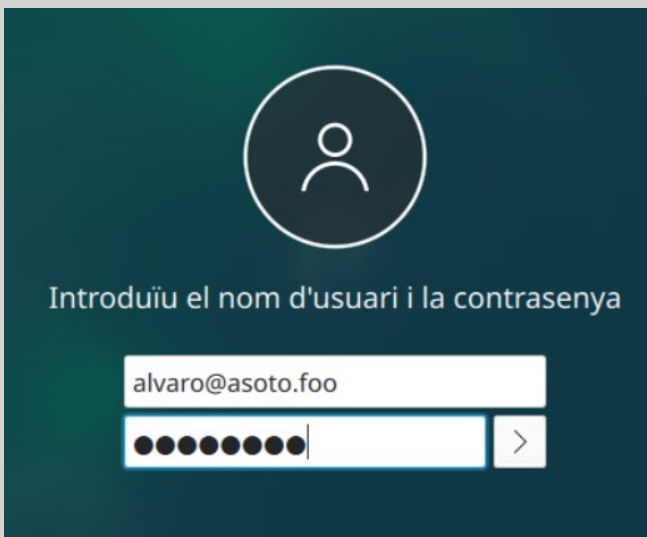
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creant el directori '/home/alvaro@asoto.foo'.
alvaro@asoto.foo@cliente-v:~$
```

Veiem que s'ha creat un directori home per a l'usuari.

```
alvaro@asoto.foo@cliente-v:~$ pwd
/home/alvaro@asoto.foo
```

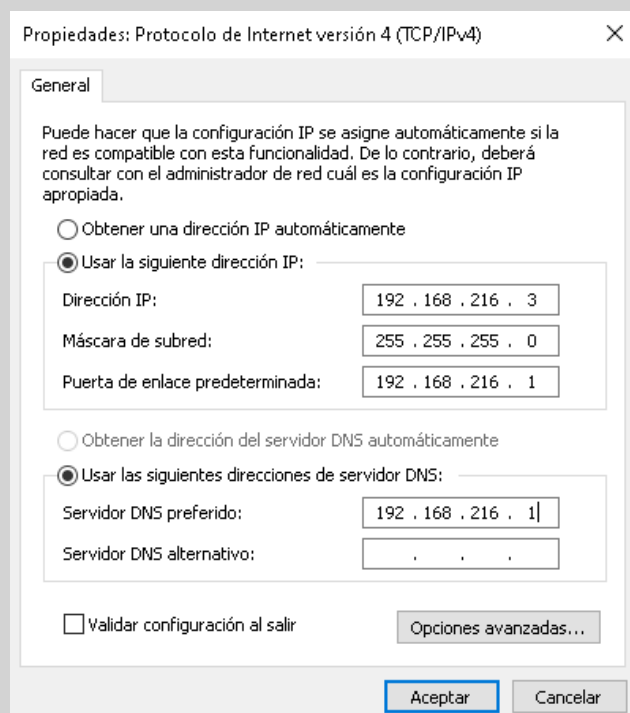
Ara també podem iniciar sessió gràficament.



## 3.2. Configuració client Windows

### 3.2.1. Configuració de xarxa

Primer configurem la xarxa.



Comprovem la connexió.

```
C:\Users\isard>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Instancia de Ethernet 0:

    Sufixo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.168.123.136
    Máscara de subred . . . . . : 255.255.252.0
    Puerta de enlace predeterminada . . . . . : 192.168.120.1

Adaptador de Ethernet Instancia de Ethernet 0 2:

    Sufixo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.168.216.3
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.216.1
```



```
C:\Users\isard>ping 192.168.216.1

Haciendo ping a 192.168.216.1 con 32 bytes de datos:
Respuesta desde 192.168.216.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.216.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.216.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.216.1: bytes=32 tiempo=2ms TTL=64

Estadísticas de ping para 192.168.216.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 2ms, Media = 2ms
```

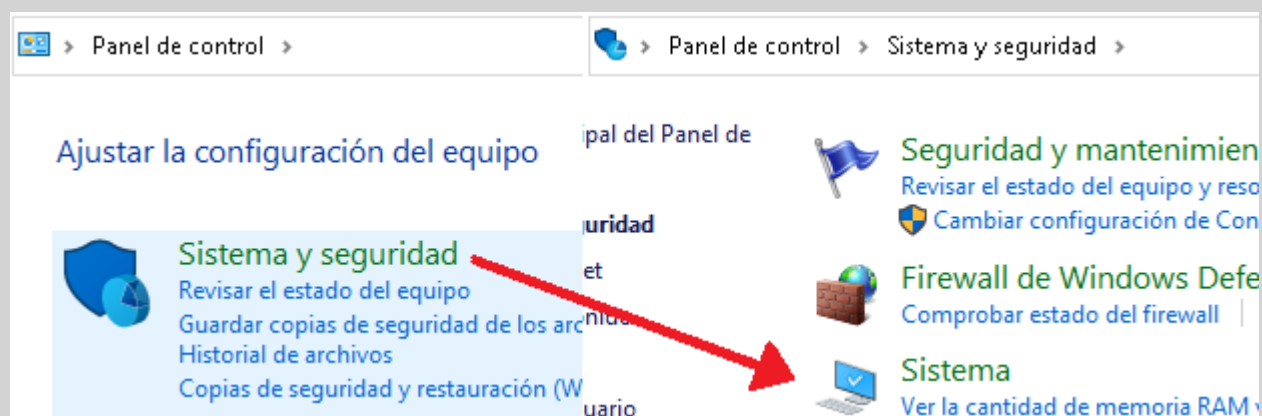
```
C:\Users\isard>ping asoto.foo

Haciendo ping a asoto.foo [192.168.216.1] con 32 bytes de datos:
Respuesta desde 192.168.216.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.216.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.216.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.216.1: bytes=32 tiempo=2ms TTL=64

Estadísticas de ping para 192.168.216.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 2ms, Media = 2ms
```

### 3.2.2. Configuració de domini

Per a afegir el client Windows al domini, anem a **Panel de Control > Sistema y Seguridad > Sistema**.



Anem fins al final de la pantalla que se'ns obre i fem clic en **Cambiar el nombre de este equipo (Avanzado)**.

## Opciones de configuración relacionadas

[Configuración de BitLocker](#)

[Administrador de dispositivos](#)

[Escritorio remoto](#)

[Protección del sistema](#)

[Configuración avanzada del sistema](#)

[Cambiar el nombre de este equipo \(avanzado\)](#)

Ara fem clic en **Cambiar**.

Para cambiar el nombre de este equipo o cambiar el dominio o grupo de trabajo, haga clic en Cambiar.

Cambiar...

Canviem el nom de màquina i el domini i fem clic a **Aceptar**.

Cambios en el dominio o el nombre del equipo X

Puede cambiar el nombre y la pertenencia de este equipo. Los cambios podrían afectar al acceso a los recursos de red.

Nombre de equipo:  
cliente-j

Nombre completo de equipo:  
cliente-j

Más...

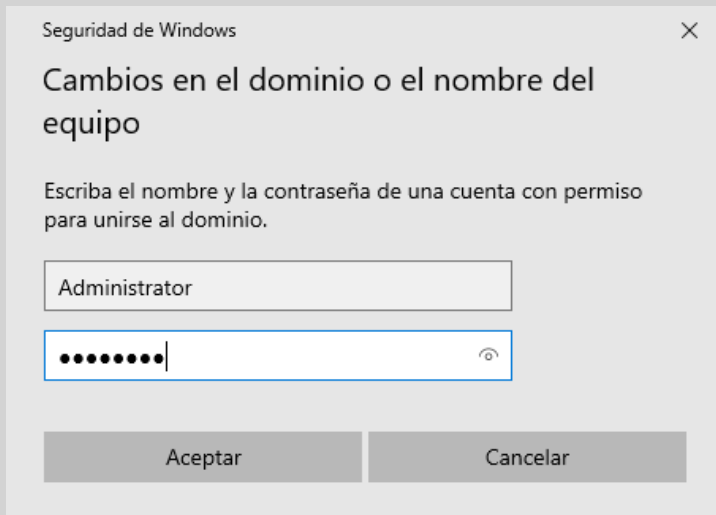
Miembro del

☒ Dominio:  
asoto.fod

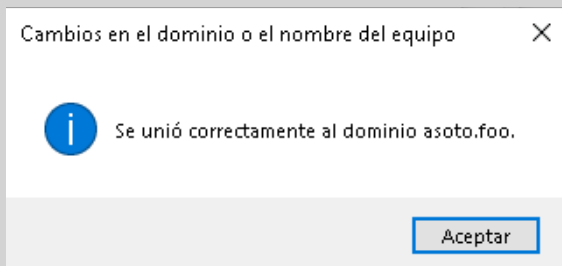
☐ Grupo de trabajo:  
WORKGROUP

Aceptar Cancelar

Ens demana usuari i contrasenya d'un compte d'administrador de domini, els introduïm i fem clic a **Aceptar**.

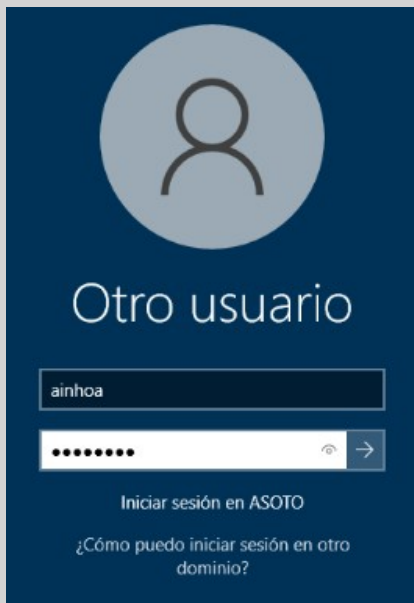


Després d'esperar una estona, se'ns afegeix la màquina correctament al domini.

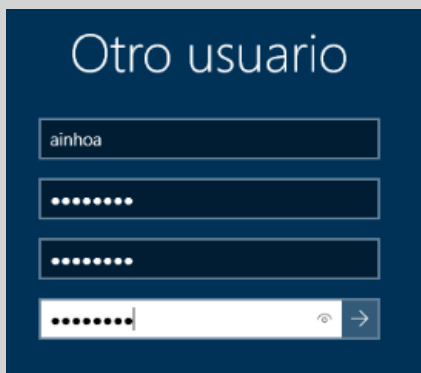
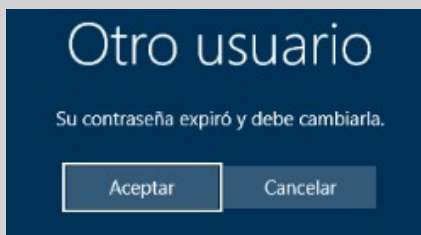


Per a aplicar els canvis, hem de reiniciar l'equip.

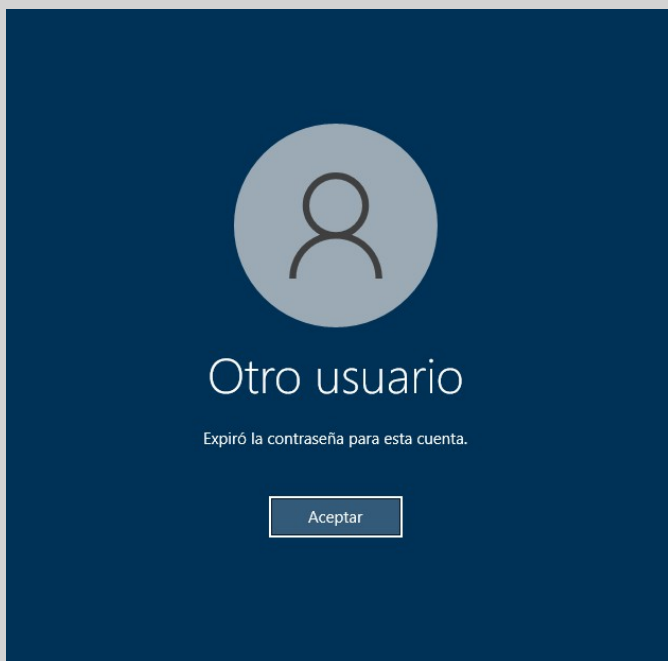
Quan es torna a iniciar Windows, provem d'iniciar sessió amb un usuari del domini.



Veiem que ens demana canviar la contrasenya.



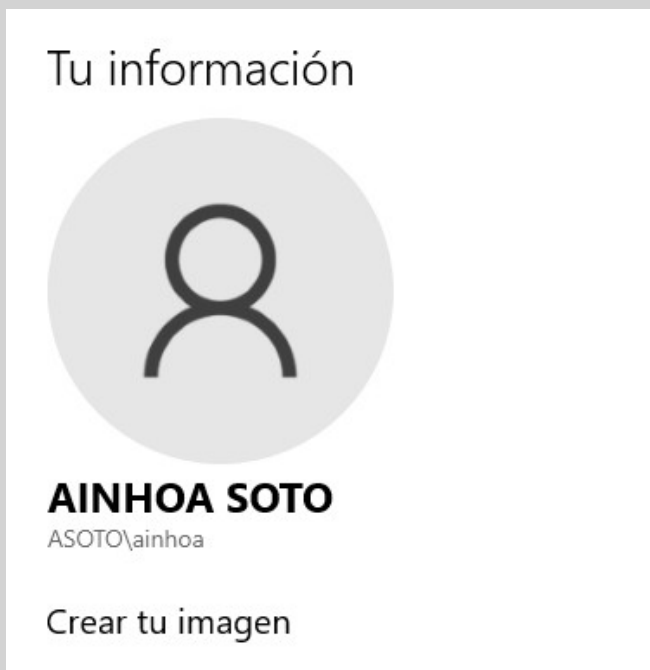
Al fer-ho, ens surt un missatge dient que la contrasenya ha expirat.



Per a solucionar això, podem canviar la contrasenya del compte deshabilitant que es canviï en el pròxim inici de sessió.

```
changed password OK
[asoto@ad-cyn ~]$ sudo samba-tool user setpassword --filter=samaccountname=ainhoa --newpassword=P@ssw0rd
[sudo] contraseña para asoto:
Changed password OK
```

Ara veiem que podem iniciar sessió correctament.

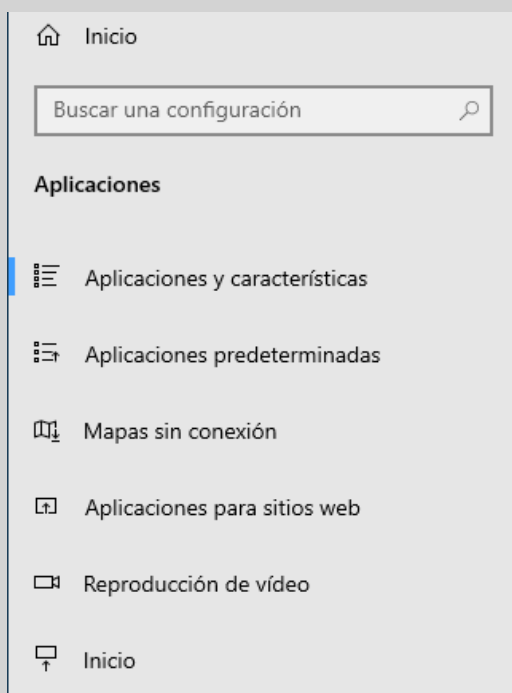


## 4. Administració de AD Samba des de Windows

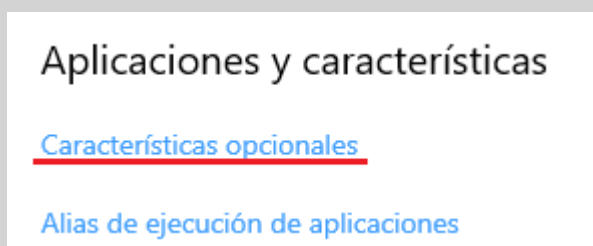
Les RSAT (Remote Server Administration Tools) ens permeten administrar un Active Directory des d'un client Windows. En el nostre cas ens permetrà tractar el nostre AD Samba com si fos un AD de Windows.

### 4.1. Instal·lació RSAT

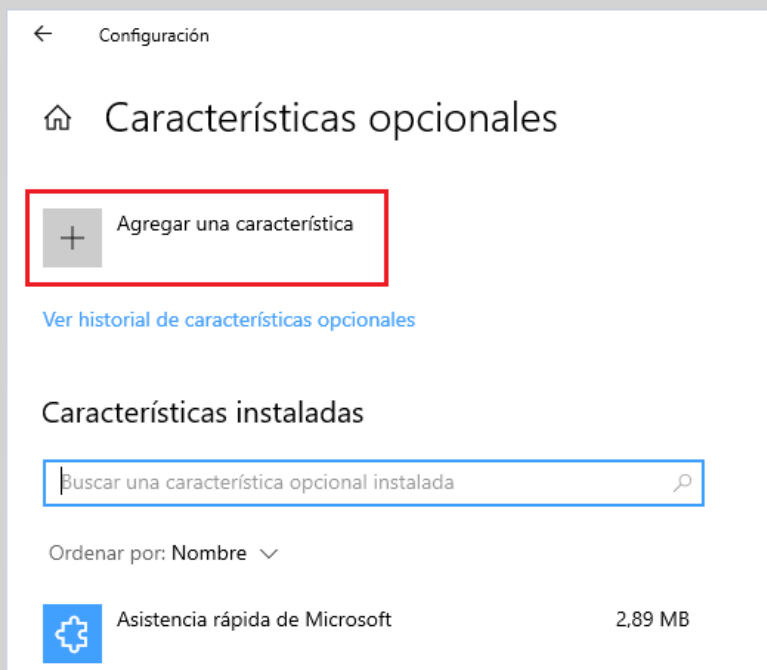
Per a instal·lar RSAT, primer anem a **Configuració > Aplicacions > Aplicacions i característiques**.



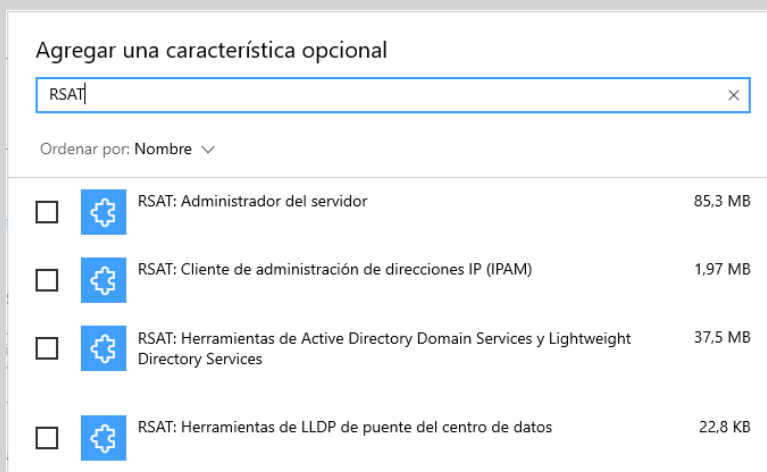
Aquí fem clic en **Características opcionales**



Fem clic en **Agregar una característica**



Busquem «RSAT», seleccionem tots els paquets per a instal·lar-los i fem clic en **Instalar**.




Una vegada instal·lades, podem administrar varies funcionalitats del servidor. Podem, per exemple, administrar els usuaris i grups.

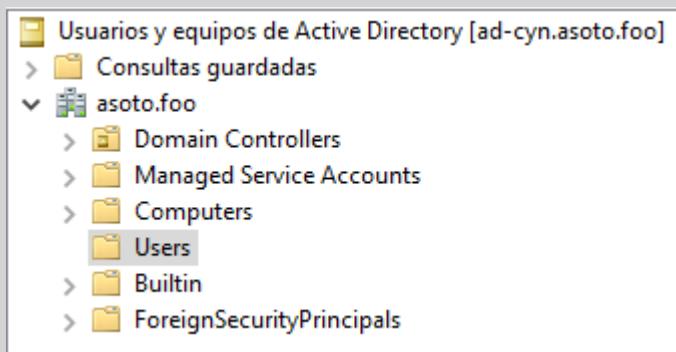


## Usuarios y equipos de Active Directory

Aplicació

 Obre

Naveguem fins a la carpeta **Users**



Aquí veiem un llistat dels usuaris i grups que existeixen al domini, podem veure que estan els dos usuaris que vam crear nosaltres.



Administrator	User	Built-in account for ad...
Allowed RODC Password Replication Group	Grupo de segu...	Members in this group c...
Protected Users	Grupo de segu...	Members of this group ...
Domain Admins	Grupo de segu...	Designated administrato...
Group Policy Creator Owners	Grupo de segu...	Members in this group c...
ainhua	User	
Denied RODC Password Replication Group	Grupo de segu...	Members in this group c...
Guest	User	Built-in account for gue...
RAS and IAS Servers	Grupo de segu...	Servers in this group can...
DnsUpdateProxy	Grupo de segu...	DNS clients who are per...
hermanos	Grupo de segu...	
Enterprise Read-only Domain Controllers	Grupo de segu...	Members of this group ...
alvaro	User	
uzi	User	
Domain Computers	Grupo de segu...	All workstations and ser...
DnsAdmins	Grupo de segu...	DNS Administrators Gro...
Domain Users	Grupo de segu...	All domain users
Domain Guests	Grupo de segu...	All domain guests
Read-only Domain Controllers	Grupo de segu...	Members of this group ...
Schema Admins	Grupo de segu...	Designated administrato...
Domain Controllers	Grupo de segu...	All domain controllers i...
Enterprise Admins	Grupo de segu...	Designated administrato...
Cert Publishers	Grupo de segu...	Members of this group ...

Podem comprovar que funciona cerant un usuari des del client windows

Nuevo objeto: User

Crear en: asoto.foo/Users

Nombre de pila: Usuario Iniciales:

Apellidos: Windows

Nombre completo: Usuario Windows

Nombre de inicio de sesión de usuario: winusr @asoto.foo

Nombre de inicio de sesión de usuario (anterior a Windows 2000): ASOTO\ winusr

< Atrás **Siguiente >** Cancelar

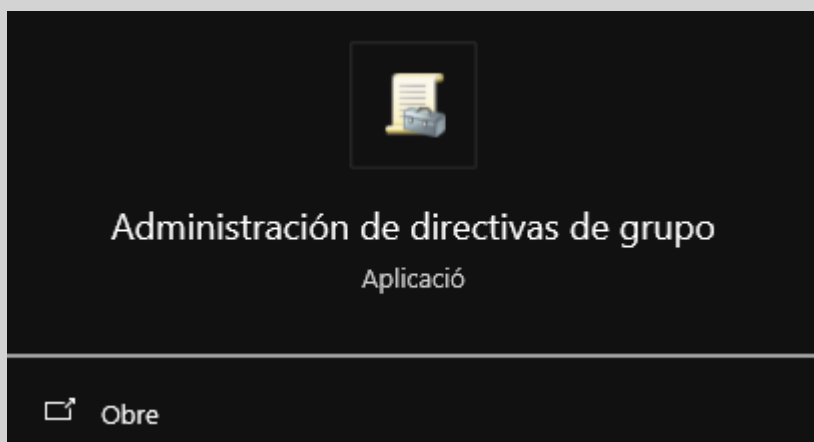
i veient que es crea en el servidor samba.

```
[asoto@ad-cyn ~]$ sudo pdbedit -L
[sudo] contraseña para asoto:
Administrator:4294967295:
CLIENTE-J$:4294967295:
CLIENTE-V$:4294967295:
ainhoa:4294967295:Ainhua Soto
nobody:65534:Kernel Overflow User
krbtgt:4294967295:
winusr:4294967295:Usuario Windows
alvaro:4294967295:Alvaro Soto
uzi:4294967295:
AD-CYN$:4294967295:
```

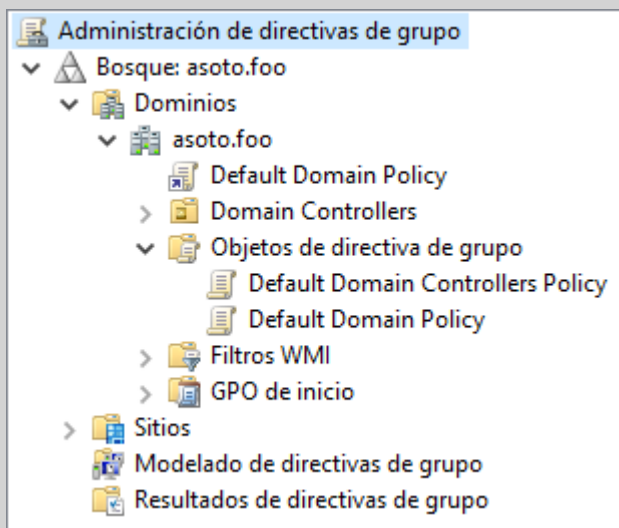
## 4.3 Creació de GPOs

Ara crearem dues GPOs

Primer obrim l'administrador de directives de grup



Al menú de la dreta, naveguem fins a **Objetos de directiva de grupo**



### 4.3.1 GPO perfil mòbil

Crearem una GPO per a habilitar el perfil mòbil als usuaris que iniciïn sessió al client Windows

Primer compartim la carpeta en samba editant l'arxiu smb.conf

```
[asoto@ad-cyn ~]$ sudo vim /etc/samba/smb.conf
```

```
[perfiles]
comment = Perfils mòbils d'usuari
path = /srv/samba/perfiles
;browseable = no
read only = no
csc policy = disable
vfs objects = acl_xattr
```

Reiniciem el servei samba i comprovem que la carpeta s'ha compartit

```
[asoto@ad-cyn ~]$ sudo systemctl reload samba.service
[asoto@ad-cyn ~]$ sudo systemctl status samba
● samba.service - Samba AD Daemon
   Loaded: loaded (/usr/lib/systemd/system/samba.service; enabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
   Active: active (running) since Tue 2024-03-19 18:52:16 CET; 53min ago
     Docs: man:samba(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 3372 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
 Main PID: 1603 (samba)
   Status: "samba: ready to serve connections..."
    Tasks: 53 (limit: 9475)
  Memory: 521.6M
    CPU: 4min 4.174s
   CGroup: /system.slice/samba.service
```

```
[asoto@ad-cyn ~]$ sudo testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_ACTIVE_DIRECTORY_DC

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

```
[perfiles]
comment = Perfils mòbils d'usuari
csc policy = disable
path = /srv/samba/perfiles
read only = No
vfs objects = acl_xattr
```

Creem un grup amb l'opció `--gid-number` i l'afegim al grup Domain Admins per a poder fer-lo servir en els permisos de la carpeta compartida.

```
[root@ad-cyn asoto]# sudo samba-tool group add "Linux Admins" \
> --nis-domain=asoto \
> --gid-number=10000
Added group Linux Admins
```

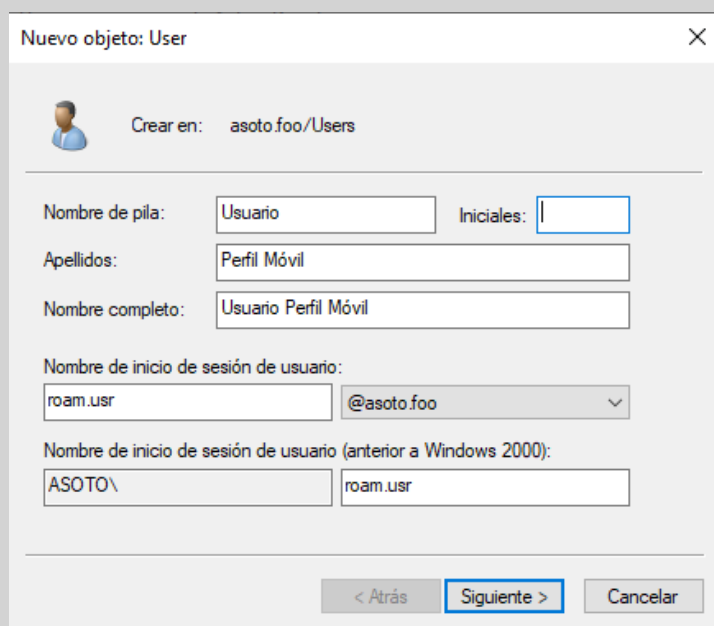
```
[root@ad-cyn asoto]# sudo samba-tool group addmembers "Domain Admins" "Linux Admins"
Added members to group Domain Admins
```

canviem els permisos de la carpeta en local i assignem el grup Domain Admins com a grup propietari

```
[asoto@ad-cyn ~]$ sudo mkdir -p /srv/samba/perfils  
[sudo] contraseña para asoto:  
[asoto@ad-cyn ~]$ sudo chmod 0770 /srv/samba/perfils
```

```
[asoto@ad-cyn ~]$ sudo chown root:"Linux Admins" /srv/samba/perfils  
chown: grupo inválido: «root:Linux Admins»
```

Creem un usuari que tindrà perfil mòbil habilitat



Nuevo objeto: User

Crear en: asoto.foo/Users

Nombre de pila: Usuario Iniciales:

Apellidos: Perfil Móvil

Nombre completo: Usuario Perfil Móvil

Nombre de inicio de sesión de usuario: roam.usr @asoto.foo

Nombre de inicio de sesión de usuario (anterior a Windows 2000): ASOTO\ roam.usr

< Atrás Siguiente > Cancelar

Profe se me crashea el explorador de Windows cuando abro la pestaña de seguridad de la carpeta perfils así no se puede

## Webgrafia

- Creació d'usuaris:  
[https://wiki.samba.org/index.php/User\\_and\\_Group\\_management#Adding\\_Users\\_into\\_Samba\\_Active\\_Directory](https://wiki.samba.org/index.php/User_and_Group_management#Adding_Users_into_Samba_Active_Directory)
- Configuració de xarxa Linux:  
<https://www.cyberciti.biz/faq/setting-up-an-network-interfaces-file/>
- Afegir client Linux al domini:  
<https://ubuntu.com/server/docs/service-sssd-ad>
- Afegir client Windows al domini:  
[https://wiki.samba.org/index.php/Joining\\_a\\_Windows\\_Client\\_or\\_Server\\_to\\_a\\_Domain](https://wiki.samba.org/index.php/Joining_a_Windows_Client_or_Server_to_a_Domain)
- Solucionar problema amb compte en Windows:  
<https://lists.samba.org/archive/samba/2018-January/213348.html>
- Crear GPO de perfil mòbil  
[https://wiki.samba.org/index.php/Roaming\\_Windows\\_User\\_Profiles#Using\\_Windows\\_ACLS](https://wiki.samba.org/index.php/Roaming_Windows_User_Profiles#Using_Windows_ACLS)