

Creación de un Samba Active Directory Domain Controller - Conexión con Windows 11

Creador: Sebastian Ariel Duarte Oruez

M4: Sistemas Operativos en Xarxa

Grupo: G4

Año: 24/25



HECHO EN MARKDOWN - OBSIDIAN

💡 *NOTA: Este documento se encuentra en mi [carpeta compartida de drive](#) y se encuentra en la dirección:*

```
/"Seguridad Informática"/EXPERIENCIA/Proyectos/Samba-AD-DC/"Creación de un Samba Active Directory Domain Controller"
```

También tenéis acceso a las imágenes en:

```
/"Seguridad Informática"/1.Imagenes/Proyectos/Samba-AD-DC
```

INDICE

- [ÍNDICE](#)
- [Pasos previos:](#)
 - [INSTALACIÓN DEL UBUNTU SERVER](#)
 - [Configuración de los adaptadores de red + IPTABLES](#)
 - [Instalación de Samba-ad-dc + Kerberos](#)
 - [Primera pantalla:](#)
 - [Segunda pantalla:](#)
 - [Tercera pantalla:](#)
 - [Configurar Samba](#)
 - [Detención de servicios](#)
 - [Configuración de resolv & hosts y activación de Samba](#)
 - [Comprobaciones](#)
 - [Confirmar que el DNS funciona](#)
 - [Comprobación de Kerberos](#)
 - [Posibles errores en la configuración](#)
 - [Creación de una carpeta compartida](#)
 - [Creación de la carpeta](#)
 - [Configuración smb.conf](#)
 - [Creación de un script para el dominio](#)
- [INSTALACIÓN Y CONFIGURACIÓN DEL WIN11 CLIENTE](#)
 - [Instalación del Windows](#)
 - [Configuración de la red y comprobación de conexión](#)
 - [Conexión al dominio](#)
 - [Posibles errores de conexión al dominio:](#)
 - [Instalación de las RSAT](#)
 - [Selección del servidor para administrar](#)
 - [Creación de un grupo de seguridad y un usuario](#)
 - [Verificación de visibilidad de la carpeta compartida](#)
 - [Configuración del script de inicio de sesión](#)

Pasos previos:

Se requiere la configuración de la interfaz de red de las máquinas virtuales en adaptador NAT y adaptador a Red Interna

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4


☒ Habilitar adaptador de red

Conectado a: NAT

Nombre:

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 0800278578BF 

☒ Cable conectado

Renvío de puertos

Red

Adaptador 1 Adaptador 2 Adaptador 3 Adaptador 4


☒ Habilitar adaptador de red

Conectado a: Red interna

Nombre: intnet

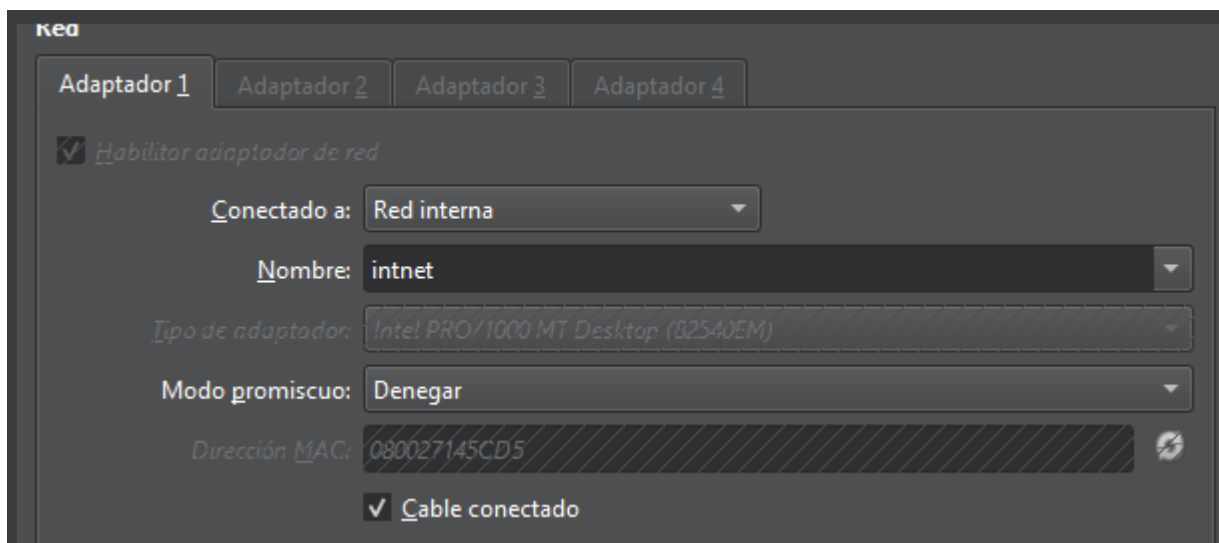
Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 08002781F993 

☒ Cable conectado

WINDOWS 11 CLIENT CONFIGURATION



INSTALACIÓN DEL UBUNTU SERVER

Para la instalación de ambas máquinas, utilizaremos VirtualBox. Al tener 2 adaptadores, nos saldrá en la configuración de red que el adaptador **enp0s8** está deshabilitado y que deberemos de configurarlo más adelante.

```
Network configuration

Configure al menos una interfaz para que este sistema sea
suficiente para las actualizaciones.

NAME      TYPE      NOTES
[ enp0s3   eth      -           ► ]
DHCPv4     10.0.2.15/24
08:00:27:85:78:bf / Intel Corporation / 82540

[ enp0s8   eth      -           ► ]
disabled  autoconfiguration failed
08:00:27:81:f9:93 / Intel Corporation / 82540

[ Create bond ► ]
```

Deberemos de seleccionar que la instalación se haga en el disco que le hemos asignado. He aquí un resumen de la instalación.

Storage configuration

RESUMEN DEL SISTEMA DE ARCHIVOS

PUNTO DE MONTAJE	TAMAÑO	TIPO	TIPO DE DISPOSITIVO
[/	11.496G	new ext4	new LVM logical volume ▶]
[/boot	2.000G	new ext4	new partition of disco local ▶]

DISPOSITIVOS DISPONIBLES

DISPOSITIVO	TIPO	TAMAÑO
[ubuntu-vg (new)	LVM volume group	22.996G ▶]
espacio disponible		11.500G ▶]
[Create software RAID (md) ▶]		
[Crear grupo de volúmenes (LVM) ▶]		

DISPOSITIVOS UTILIZADOS

DISPOSITIVO	TIPO	TAMAÑO
[ubuntu-vg (new)	LVM volume group	22.996G ▶]
ubuntu-lv	new, to be formatted as ext4, mounted at /	11.496G ▶]
[VBOX_HARDDISK_VB32740c26-b7dc42d9	disco local	25.000G ▶]
partition 1	new, BIOS grub spacer	1.000M ▶]
partition 2	new, to be formatted as ext4, mounted at /boot	2.000G ▶]
partition 3	new, PV of LVM volume group ubuntu-vg	22.997G ▶]

También, configuraremos un usuario y el hostname:

```
user: carpi
password: 12345
hostname: smb4duarte
```

Enter the username and password you will use to log in to the system. You can configure SSH access on a later screen, but a password is still needed for sudo.

Su nombre: carpi

Your servers name: smb4duarte

The name it uses when it talks to other computers.

Elija un nombre de usuario: carpi

Elija una contraseña: *****

Confirme la contraseña: *****

Configuración de los adaptadores de red + IPTABLES

Para la configuración de la red interna, utilizaremos el adaptador `enp0s8`. Deberemos de ir al archivo de configuración de netplan con el siguiente prompt:

```
cd /etc/netplan/
nvim [TAB]
```

```

network:
  version: 2
  ethernet:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses:
        - 192.168.0.1/24

```

Aquí estaremos configurando que el adaptador **enp0s8** tenga la dirección IP 192.168.0.1/24. Para aplicar la configuración:

```
sudo netplan apply
```

Para verificar que se ha configurado correctamente:

```
ip a
```

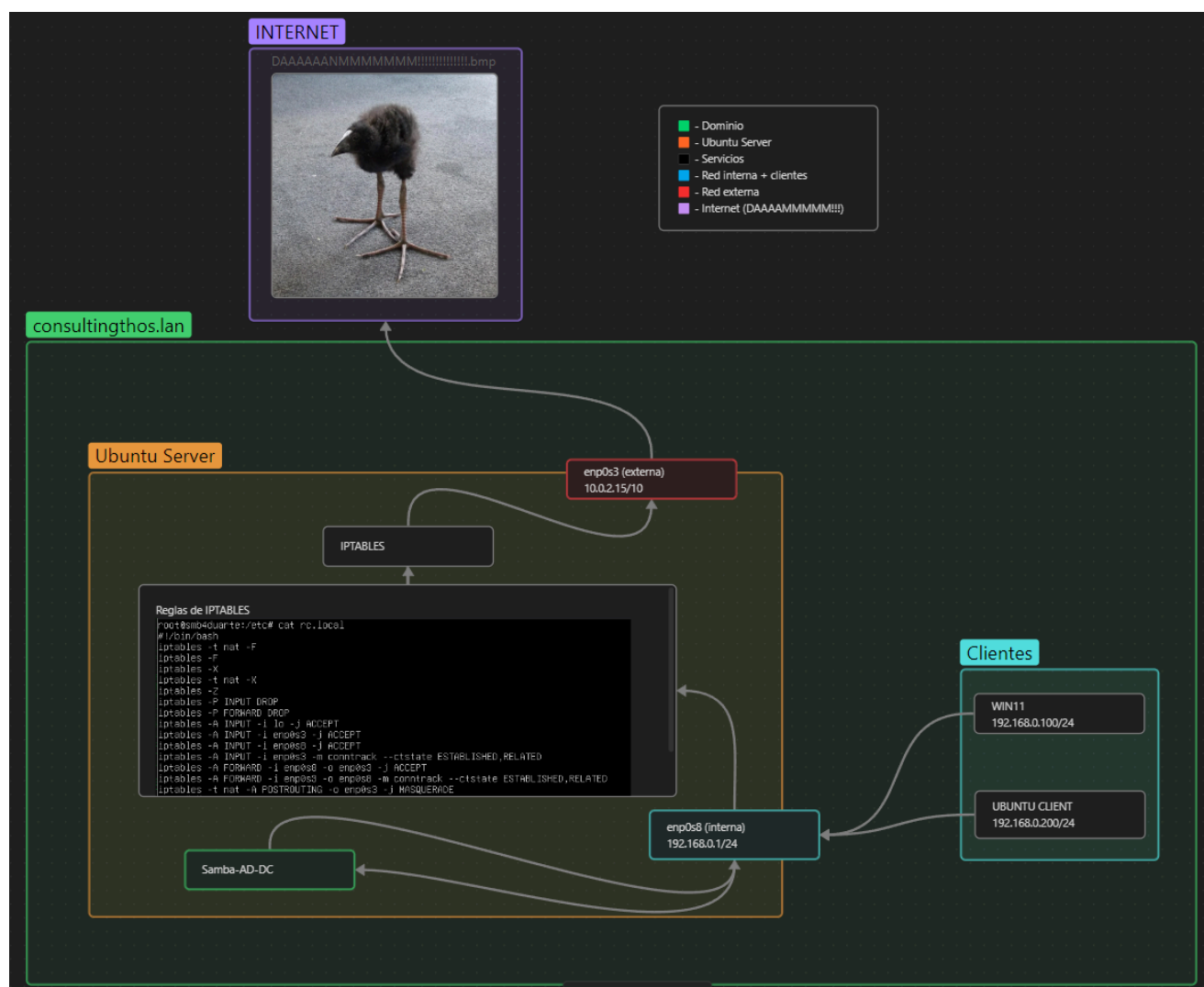
```

root@smb4duarte:/etc# netplan apply
root@smb4duarte:/etc# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:85:78:bf brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86399sec preferred_lft 86399sec
    inet6 fd17:625c:f037:2:a00:27ff:fe85:78bf/64 scope global tentative dynamic mngtmpaddr noprefixroute
        valid_lft 86400sec preferred_lft 14400sec
    inet6 fe80::a00:27ff:fe85:78bf/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:81:f9:93 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.1/24 brd 192.168.0.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe81:f993/64 scope link
        valid_lft forever preferred_lft forever
root@smb4duarte:/etc#

```

Aquí podemos ver que el adaptador **enp0s8** ahora sí tiene una dirección IP, que es la que acabamos de configurar (color naranja).

Para que nuestras máquinas clientes posean salida a internet, deberemos de configurar IPTABLES para el redireccionamiento entre adaptadores. E aquí un esquema de lo que se quiere conseguir:



- - Dominio
- - Ubuntu Server
- - Servicios
- - Red interna + clientes
- - Red externa
- - Internet

Tenemos los clientes conectados al adaptador **enp0s8** y queremos que IPTABLES redireccione todas las peticiones hacia el adaptador **enp0s3** (la NAT). Para ello, en **/etc/**, podemos colocar el script **rc.local**.

Crearemos el fichero en la dirección correspondiente y le daremos permisos de ejecución con el siguiente comando:

```
touch rc.local
chmod +x rc.local
```

Ahora, editaremos el fichero y pondremos lo siguiente:

```
#!/bin/bash
iptables -t nat -F
iptables -F
iptables -X
iptables -t nat -X
iptables -Z
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i enp0s3 -j ACCEPT
iptables -A INPUT -i enp0s8 -j ACCEPT
iptables -A INPUT -i enp0s3 -m conntrack --ctstate ESTABLISHED,RELATED
iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -m conntrack --ctstate
ESTABLISHED,RELATED
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward
ufw disable
exit 0
```

```
root@smb4duarte:/etc# cat rc.local
#!/bin/bash
iptables -t nat -F
iptables -F
iptables -X
iptables -t nat -X
iptables -Z
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i enp0s3 -j ACCEPT
iptables -A INPUT -i enp0s8 -j ACCEPT
iptables -A INPUT -i enp0s3 -m conntrack --ctstate ESTABLISHED,RELATED
iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -m conntrack --ctstate ESTABLISHED,RELATED
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward
ufw disable
exit 0
```

He de resaltar que en la línea 15 se encuentra:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Esto nos servirá para aceptar las redirecciones de IPTABLES.

Ejecutamos:

```
root@smb4duarte:/etc# chmod +x rc.local
root@smb4duarte:/etc# ./rc.local
Firewall stopped and disabled on system startup
root@smb4duarte:/etc#
```

Y si no nos da ningún tipo de error, estamos bien. Si eso ocurre, revisa la sintaxis del fichero.

Instalación de Samba-ad-dc + Kerberos

Antes de nada deberemos de actualizar la máquina con el siguiente comando:

```
sudo apt update -y && sudo apt upgrade -y && sudo apt dist-upgrade -y
```

Una vez actualizados, instalaremos los siguientes paquetes:

```
sudo apt install samba krb5-config winbind smbclient -y
```

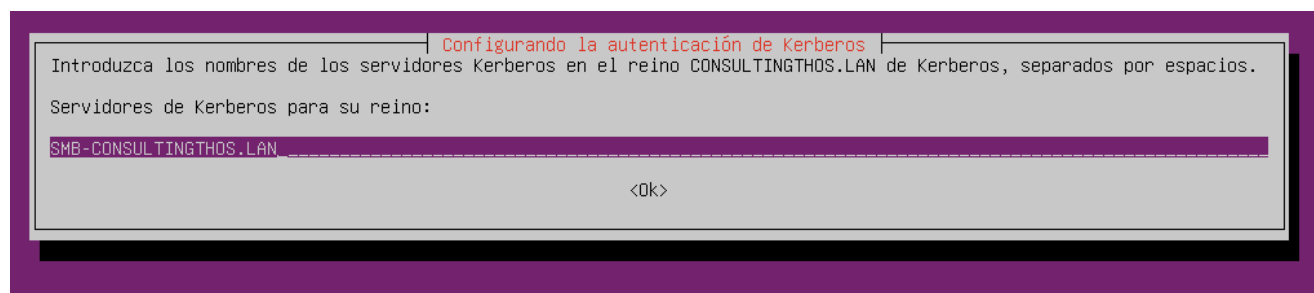
Cuando nos llegue el momento de instalar **Kerberos**, nos pedirá el **REALM**. En realidad se refiere al nombre del dominio, y en nuestro caso es CONSULTINGTHOS.LAN (NOTA: toda la configuración del kerberos va en mayúsculas).

Primera pantalla:

```
REALM = CONSULTINGTHOS.LAN
```

Después, el instalador nos solicita el nombre de los *servidores de Kerberos para nuestro reino*. En este caso, se refiere a los controladores de dominio que tengamos definidos. En este caso, solo tenemos uno y se llama SMB-CONSULTINGTHOS.LAN

Segunda pantalla:



Configurando la autenticación de Kerberos

Introduzca los nombres de los servidores Kerberos en el reino CONSULTINGTHOS.LAN de Kerberos, separados por espacios.

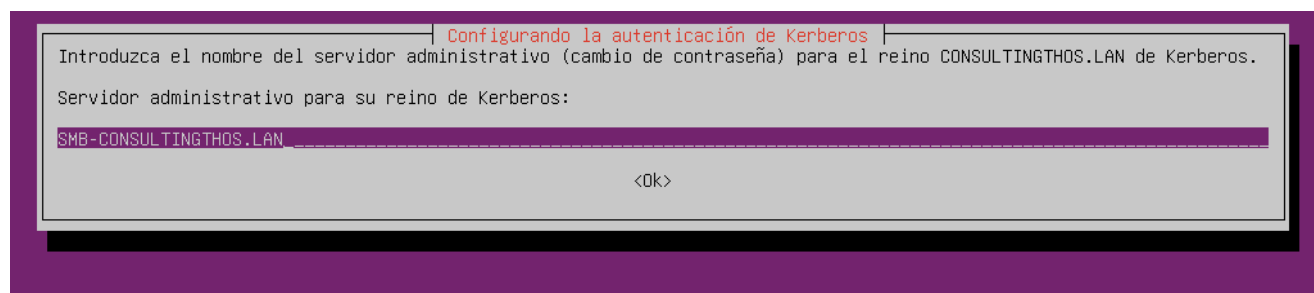
Servidores de Kerberos para su reino:

SMB-CONSULTINGTHOS.LAN

<Ok>

Por último, nos solicita el *servidor administrativo para nuevo reino de Kerberos*. Volvemos a escribir el nombre SMB-CONSULTINGTHOS.LAN

Tercera pantalla:



Configurando la autenticación de Kerberos

Introduzca el nombre del servidor administrativo (cambio de contraseña) para el reino CONSULTINGTHOS.LAN de Kerberos.

Servidor administrativo para su reino de Kerberos:

SMB-CONSULTINGTHOS.LAN

<Ok>

Después de esto, la instalación continuará por algunos segundos más, pero ya no se necesita ningún aporte de información.

Configurar Samba

Antes de continuar con la configuración, debemos de cambiar de sitio el archivo *smb.conf* que contiene la configuración predeterminada.

Para cambiar el nombre del archivo, deberemos de escribir lo siguiente:

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

Ahora, ya podremos proseguir con la configuración.

Utilizaremos la herramienta *samba-tool* para configurar samba:

```
sudo samba-tool domain provision
```

Se nos pedirá el **realm** (es el nombre en mayúsculas del dominio usado por Kerberos), **domain** (es el NetBIOS domain name, usado por Samba), **server role**, **DNS backend** y **DNS forwarder**. Deberemos de introducir lo siguiente en cada caso:

- **Realm:** CONSULTINGTHOS.LAN
- **DOMAIN:** CONSULTINGTHOS
- **SERVER ROLE:** dc
- **DNS backend:** SAMBA_INTERNAL
- **DNS forwarder:** 8.8.8.8

Además de la contraseña para el usuario "administrator".

```
root@smb4duarte:/etc# samba-tool domain provision
Realm:  CONSULTINGTHOS.LAN
Domain [CONSULTINGTHOS]:
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:
```

Después de eso, comenzará a hacer algunas acciones y al finalizar nos ofrecerá un pequeño resumen de la configuración:

```
INFO 2025-04-18 18:49:24,129 pid:16794 /usr/lib/python3/dist-packages/samba/provision/__init__.py #499: Hostname: smb4duarte
INFO 2025-04-18 18:49:24,129 pid:16794 /usr/lib/python3/dist-packages/samba/provision/__init__.py #500: NetBIOS Domain: CONSULTINGTHOS
INFO 2025-04-18 18:49:24,129 pid:16794 /usr/lib/python3/dist-packages/samba/provision/__init__.py #501: DNS Domain: consultingthos.lan
INFO 2025-04-18 18:49:24,129 pid:16794 /usr/lib/python3/dist-packages/samba/provision/__init__.py #502: DOMAIN SID: S-1-5-21-3933829533-1156820038-156348423
root@smb4duarte:/etc# _
```

Con esto, además de configurarse *Samba*, también se ha generado un archivo de configuración para *Kerberos* en la ruta `/var/lib/samba/private/krb5.conf`.

Deberemos de copiarlo a `/etc/` con:

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

```
root@smb4duarte:/etc# cp /var/lib/samba/private/krb5.conf /etc/
root@smb4duarte:/etc#
```

Detención de servicios

Lo siguiente será ajustar la resolución de nombres, y comenzaremos deteniendo y deshabilitando los servicios implicados:

```
sudo systemctl stop smbd nmbd winbind systemd-resolved && \
sudo systemctl disable smbd nmbd winbind systemd-resolved
```

```
root@smb4duarte:/etc# sudo systemctl stop smbd nmbd winbind systemd-resolved
root@smb4duarte:/etc# sudo systemctl disable smbd nmbd winbind systemd-resolved
Synchronizing state of smbd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable smbd
Synchronizing state of nmbd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable nmbd
Synchronizing state of winbind.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable winbind
Removed "/etc/systemd/system/dbus-org.freedesktop.resolve1.service".
Removed "/etc/systemd/system/sysinit.target.wants/systemd-resolved.service".
Removed "/etc/systemd/system/smb.service".
Removed "/etc/systemd/system/nmb.service".
Removed "/etc/systemd/system/multi-user.target.wants/smbd.service".
Removed "/etc/systemd/system/multi-user.target.wants/winbind.service".
Removed "/etc/systemd/system/multi-user.target.wants/nmbd.service".
root@smb4duarte:/etc# _
```

A continuación, nos aseguramos de que el servicio *samba-ad-dc* se podrá iniciar sin problemas, evitando cualquier enmascaramiento que pueda existir:

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

```
root@smb4duarte:/etc# sudo systemctl unmask samba-ad-dc
root@smb4duarte:/etc# _
```

Configuración de resolv & hosts y activación de Samba

Ahora, deberemos de eliminar el archivo *resolv.conf* que, en realidad, es un enlace a `../run/systemd/resolve/stub-resolv.conf`. Podemos comprobarlo con:

```
sudo ls -l /etc/resolv.conf
```

```
root@smb4duarte:/etc# sudo ls -l /etc/resolv.conf
lrwxrwxrwx 1 root root 39 feb 16 20:58 /etc/resolv.conf -> ../run/systemd/resolve/stub-resolv.conf
root@smb4duarte:/etc#
```

Borramos el archivo y creamos uno nuevo para editarlo con:

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

```
root@smb4duarte:/etc# sudo rm /etc/resolv.conf
root@smb4duarte:/etc# sudo nvim /etc/resolv.conf
```

Una vez dentro, deberemos de introducir lo siguiente:

```
domain smb.consultingthos.lan
nameserver 127.0.0.1
```

```
domain smb.consultingthos.lan
nameserver 127.0.0.1
```

Guarda y sal.

El archivo `/etc/hosts` tiene la relación de direcciones IP con sus correspondientes nombres lógicos. Cuando hagamos referencia a un ordenador que esté identificado en esta lista, el acceso es inmediato, algo así como un DNS integrado.

Este archivo contiene una referencia al nombre del propio servidor y le deberemos de añadir tanto el nombre DNS como el nombre *NetBIOS* (`smb-consultingthos.lan` y `smb`) con su respectiva IP estática (la dirección interna del servidor, `192.168.0.1`):

```
127.0.0.1 localhost
127.0.1.1 smb4duarte
127.0.0.1 smb.consultingthos.lan smb
192.168.0.1 smb.consultingthos.lan smb
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

solo nos queda iniciar el servicio samba y habilitarlo

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

```
root@smb4duarte:/etc# sudo systemctl start samba-ad-dc
root@smb4duarte:/etc# sudo systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable samba-ad-dc
root@smb4duarte:/etc#
```

Comprobaciones

Una vez terminado, haremos las comprobaciones con `samba-tool`.

Para consultar el nivel del dominio, deberemos de introducir lo siguiente:

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

```
root@smb4duarte:/etc# samba-tool domain level show
Domain and forest function level for domain 'DC=consultingthos,DC=lan'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
root@smb4duarte:/etc#
```

Aquí, comprobamos que el nivel del dominio y del bosque donde se encuentra equivale a una instalación *Windows Server 2008 R2*.

Como parece que la instalación es correcta, probamos a crear un usuario:

```
sudo samba-tool user create usuario-prueba
```

```
root@smb4duarte:/etc# samba-tool user create usuario-prueba
New Password:
Retype Password:
User 'usuario-prueba' added successfully
root@smb4duarte:/etc#
```

Funciona, así que bien.

Confirmar que el DNS funciona

Lo primero será comprobar el servicio *LDAP* sobre el protocolo *TCP* y *Kerberos* sobre protocolo *UDP*:

```
host -t SRV _ldap._tcp.consultingthos.lan && \
host -t SRV _kerberos._udp.consultingthos.lan
```

Si todo es correcto, recibiremos lo siguiente:

```
root@smb4duarte:/etc# host -t SRV _ldap._tcp.consultingthos.lan
_ldap._tcp.consultingthos.lan has SRV record 0 100 389 smb4duarte.consultingthos.lan.
root@smb4duarte:/etc# host -t SRV _kerberos._udp.consultingthos.lan
_kerberos._udp.consultingthos.lan has SRV record 0 100 88 smb4duarte.consultingthos.lan.
root@smb4duarte:/etc#
```

Por último, toca revisar la resolución de nuestro servidor:

```
sudo host -t A consultingthos.lan
```

```
root@smb4duarte:/etc# host -t A consultingthos.lan
consultingthos.lan has address 192.168.0.1
consultingthos.lan has address 10.0.2.15
root@smb4duarte:/etc#
```

Para completar, usaremos `nslookup`.

Al ejecutar, nos aparecerá un “>”, donde podremos ir escribiendo argumentos.

Para comenzar, escribiremos el comando `server` seguido de la *dirección IP* del equipo y verificamos que resuelve bien.

Después, establecemos el tipo de consulta que utilice los registros SRV y añadimos el nombre de servicio a consultar. Al hacerlo, verificamos que también se resuelve de forma satisfactoria.

```
root@smb4duarte:/etc# nslookup
> server 192.168.0.1
Default server: 192.168.0.1
Address: 192.168.0.1#53
> set type=SRV
> _ldap._tcp.consultingthos.lan
Server:      192.168.0.1
Address:     192.168.0.1#53

_ldap._tcp.consultingthos.lan  service = 0 100 389 smb4duarte.consultingthos.lan.
> exit

root@smb4duarte:/etc#
```

Comprobación de Kerberos

Con `smbclient`, podemos comprobar los servicios que puede obtener un determinado usuario. Por ejemplo, “*administrator*”

```
sudo smbclient -L smb.consultingthos.lan -U 'administrator'
```

```

root@smb4duarte:/etc# smbclient -L smb.consultingthos.lan -U 'administrator'
Password for [CONSULTINGTHOS\administrator]:

      Sharename      Type      Comment
      -----      -
      sysvol         Disk
      netlogon       Disk
      IPC$           IPC       IPC Service (Samba 4.19.5-Ubuntu)
SMB1 disabled -- no workgroup available
root@smb4duarte:/etc#

```

Si la autenticación es correcta, ya sabremos que *Kerberos* está haciendo su trabajo.

Si queremos, incluso podemos iniciar sesión en el servidor usando la cuenta de administración:

```

sudo smbclient //localhost/netlogon -U 'administrator'

```

```

root@smb4duarte:/etc# smbclient //localhost/netlogon -U 'administrator'
Password for [CONSULTINGTHOS\administrator]:
Try "help" to get a list of possible commands.
smb: \>

```

Para concluir, utilizaremos **testparm**, el cual comprueba la integridad de la configuración de *Samba* (podemos también obtener un volcado completo del archivo pulsando **ENTER**):

```

sudo testparm

```

```

root@smb4duarte:/etc# 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

# Global parameters
[global]
    dns forwarder = 8.8.8.8
    passwd backend = samba_dsdb
    realm = CONSULTINGTHOS.LAN
    server role = active directory domain controller
    workgroup = CONSULTINGTHOS
    rpc_server:tcpip = no
    rpc_daemon:spoolssd = embedded
    rpc_server:spoolss = embedded
    rpc_server:winreg = embedded
    rpc_server:ntsvcs = embedded
    rpc_server:eventlog = embedded
    rpc_server:svcsvc = embedded
    rpc_server:svcctl = embedded
    rpc_server:default = external
    winbindd:use external pipes = true
    idmap config * : backend = tdb
    map archive = No
    vfs objects = dfs_samba4 acl_xattr

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

[netlogon]
    path = /var/lib/samba/sysvol/consultingthos.lan/scripts
    read only = No
root@smb4duarte:/etc#

```

Si has llegado hasta aquí...

Felicidades, has configurado correctamente Samba-ad-dc 🎉 🙌

Posibles errores en la configuración

- Kerberos no da tickets correctos o no los da → Verificar la zona horaria.

Creación de una carpeta compartida

Creación de la carpeta

Para crear una carpeta compartida, primero tenemos que definirla en algún sitio

En este caso, estará en la carpeta `/home`


```
mkdir /home Carpeta_compartida
chmod 777 /home/Carpeta_compartida
```

Para hacer una prueba más tarde, voy a colocar un fichero `README.txt` dentro de la carpeta:

```
echo "carpeta_compartida" > /home/Carpeta_compartida/README.txt
```

```
root@smb4duarte:/home# mkdir Carpeta_compartida
root@smb4duarte:/home# chmod 777 Carpeta_compartida/
root@smb4duarte:/home# ls
Carpeta_compartida  carpi
root@smb4duarte:/home# echo "carpeta_compartida" > Carpeta_compartida/README.txt
root@smb4duarte:/home#
```

Configuración smb.conf

Para que la carpeta sea visible desde los usuarios dentro del dominio, deberemos de ir a `/etc/samba` y añadir lo siguiente al fichero `smb.conf`:

```
[Compartit]
    path = /home/Carpeta_compartida
    comment = Carpeta compartida desde Samba AD-DC
    writable = yes
    guests ok = yes
```

```
[Compartit]
    path = /home/Carpeta_compartida
    comment = Carpeta compartida desde Samba AD-DC (lo que me ha costado llegar hasta aqui ctm.)
    browseable = yes
    writable = yes
    guest ok = yes
root@smb4duarte:/etc/samba#
```

Creación de un script para el dominio

En caso de que necesitemos crear un script de inicio de sesión para los usuarios que se administren desde un Windows como administrador, como `ROOT` deberemos de ir a la siguiente ruta:

```
cd /var/lib/samba/sysvol/consultingthos.lan/scripts
```

En este caso, crearemos un pequeño script en `bat` (Nombre: `conecta.bat`) para que cuando un usuario al cual se le haya asignado el script, conecte automáticamente la carpeta compartida de antes en la unidad Z:\

```
root@smb4duarte:/var/lib/samba/sysvol/consultingthos.lan/scripts# nvim conecta.bat
```

```
@echo off
```

```
net use z: \\smb4duarte\Compartit
```

```
@echo off
```

```
net use z: \\smb4duarte\Compartit
```

INSTALACIÓN Y CONFIGURACIÓN DEL WIN11 CLIENTE

Instalación del Windows

Para que después se puedan utilizar los RSAT, deberemos de configurar la instalación de Windows 11 PRO.

Sistema operativo:

Windows 11 Home

Windows 11 Home N

Windows 11 Home Single Language

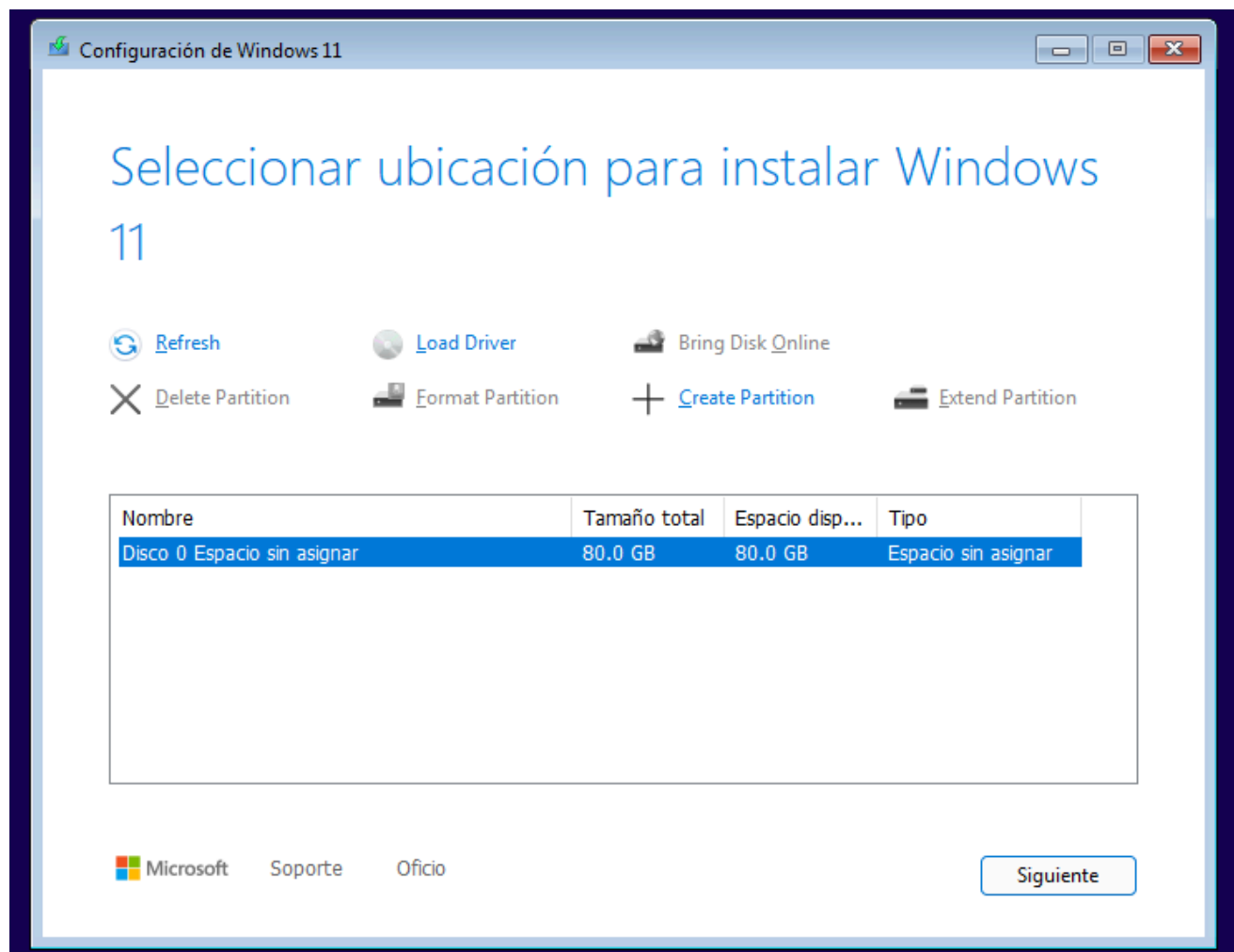
Windows 11 Education

Windows 11 Education N

Windows 11 Pro

Windows 11 Pro

Cuando lo tengamos listo, seleccionaremos el disco vacío e instalaremos.



Cuando nos aparezca la ventana de iniciar sesión con una cuenta de Microsoft, haremos lo siguiente:

Otras opciones de inicio de sesión > Conectar a dominio

Luego de esto, nos pedirá un nombre de usuario para la cuenta local. No hará falta una contraseña para el usuario si no queremos.

username: carpi
password:

¿Quién va a usar este equipo?

Usarás este nombre para iniciar sesión en el dispositivo.

Escriba su nombre

Hubo algún problema.

carpi

O, incluso mejor, usa una cuenta en línea

¿Es esta cuenta para un niño o adolescente?

Si es así, considere la posibilidad de iniciar sesión con una cuenta de Microsoft para niños.

Siguiente

Configuración de la red y comprobación de conexión

Para que los equipos (servidor y cliente) se vean entre sí, deberemos de configurar las direcciones IP y el DNS:

Configuración de Ethernet > (EDITAR)-Asignación de IP > Manual > IPv4

IP: 192.168.0.100

MASCARA: 255.255.255.0

PUERTA DE ENLACE: 192.168.0.1

DIRECCION DNS: 192.168.0.1

Asignación de IP:

Manual

Dirección IPv4:

192.168.0.100

Máscara IPv4:

255.255.255.0

Puerta de enlace de IPv4:

192.168.0.1

Editar

Asignación de servidor DNS:

Manual

Servidores DNS IPv4:

192.168.0.1 (sin cifrar)

Editar

Por si acaso, desactivaremos el *Firewall de dominio*:

Firewall y protección de red > Red de dominio > Desactivar el switch

Red de dominio

Redes del trabajo que estén unidas a un dominio.

Redes de dominio activas

No conectado

Firewall de Microsoft Defender

Ayuda a proteger el dispositivo mientras se utiliza en una red del dominio.



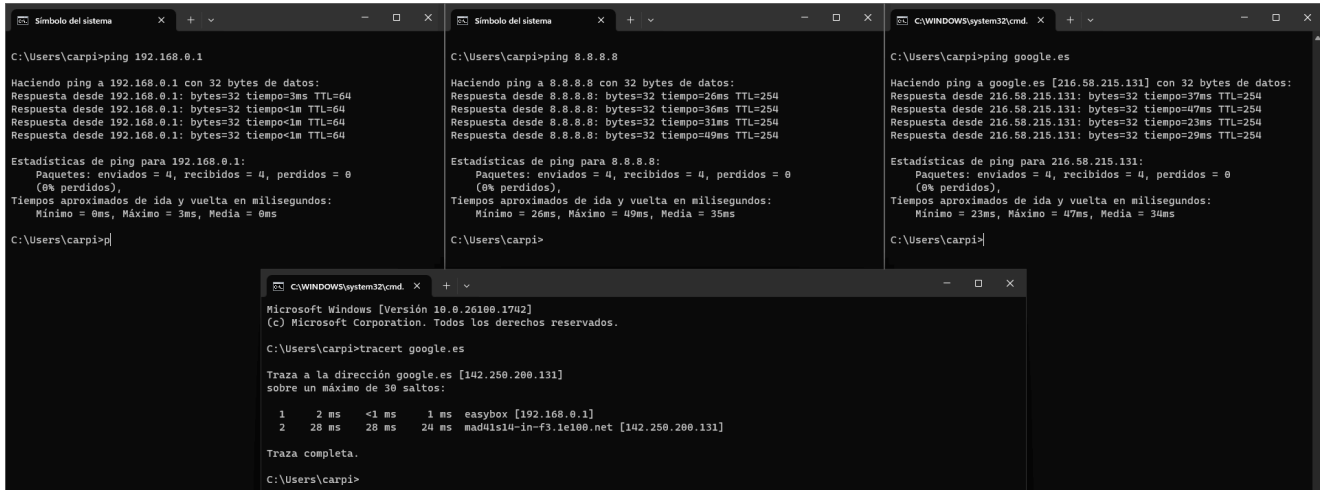
Dominio firewall está desactivado. El dispositivo puede estar en peligro.



Desactivado

Para comprobar la conectividad entre cliente/servidor y conexión a internet, abrimos el CMD (a ser posible, cada comando en un CMD distinto) y ponemos lo siguiente

```
ping 192.168.0.1
ping 8.8.8.8
ping google.es
tracert google.es
```



The image shows three separate Windows Command Prompt windows. The first window shows the results of a ping command to 192.168.0.1, indicating successful connectivity with 0% packet loss. The second window shows the results of a ping command to 8.8.8.8, also indicating successful connectivity with 0% packet loss. The third window shows the results of a ping command to google.es, indicating successful connectivity with 0% packet loss. Below these, a fourth window shows the results of a tracert command to google.es, displaying the path taken by the data packets from the local network to the destination.

```
C:\Users\carpi>ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=1m TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=1m TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=1m TTL=64

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 3ms, Media = 0ms

C:\Users\carpi>

C:\Users\carpi>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=26ms TTL=254
Respuesta desde 8.8.8.8: bytes=32 tiempo=36ms TTL=254
Respuesta desde 8.8.8.8: bytes=32 tiempo=31ms TTL=254
Respuesta desde 8.8.8.8: bytes=32 tiempo=49ms TTL=254

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 26ms, Máximo = 49ms, Media = 35ms

C:\Users\carpi>

C:\Users\carpi>ping google.es

Haciendo ping a google.es [216.58.215.131] con 32 bytes de datos:
Respuesta desde 216.58.215.131: bytes=32 tiempo=37ms TTL=254
Respuesta desde 216.58.215.131: bytes=32 tiempo=47ms TTL=254
Respuesta desde 216.58.215.131: bytes=32 tiempo=23ms TTL=254
Respuesta desde 216.58.215.131: bytes=32 tiempo=29ms TTL=254

Estadísticas de ping para 216.58.215.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 23ms, Máximo = 47ms, Media = 34ms

C:\Users\carpi>

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 10.0.26100.1702]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\carpi>tracert google.es

Traza a la dirección google.es [142.250.200.131]
sobre un máximo de 30 saltos:

  1    2 ms    <1 ms    1 ms  easybox [192.168.0.1]
  2   28 ms   28 ms   24 ms  mad4is14-in-f3.1e100.net [142.250.200.131]

Traza completa.

C:\Users\carpi>
```

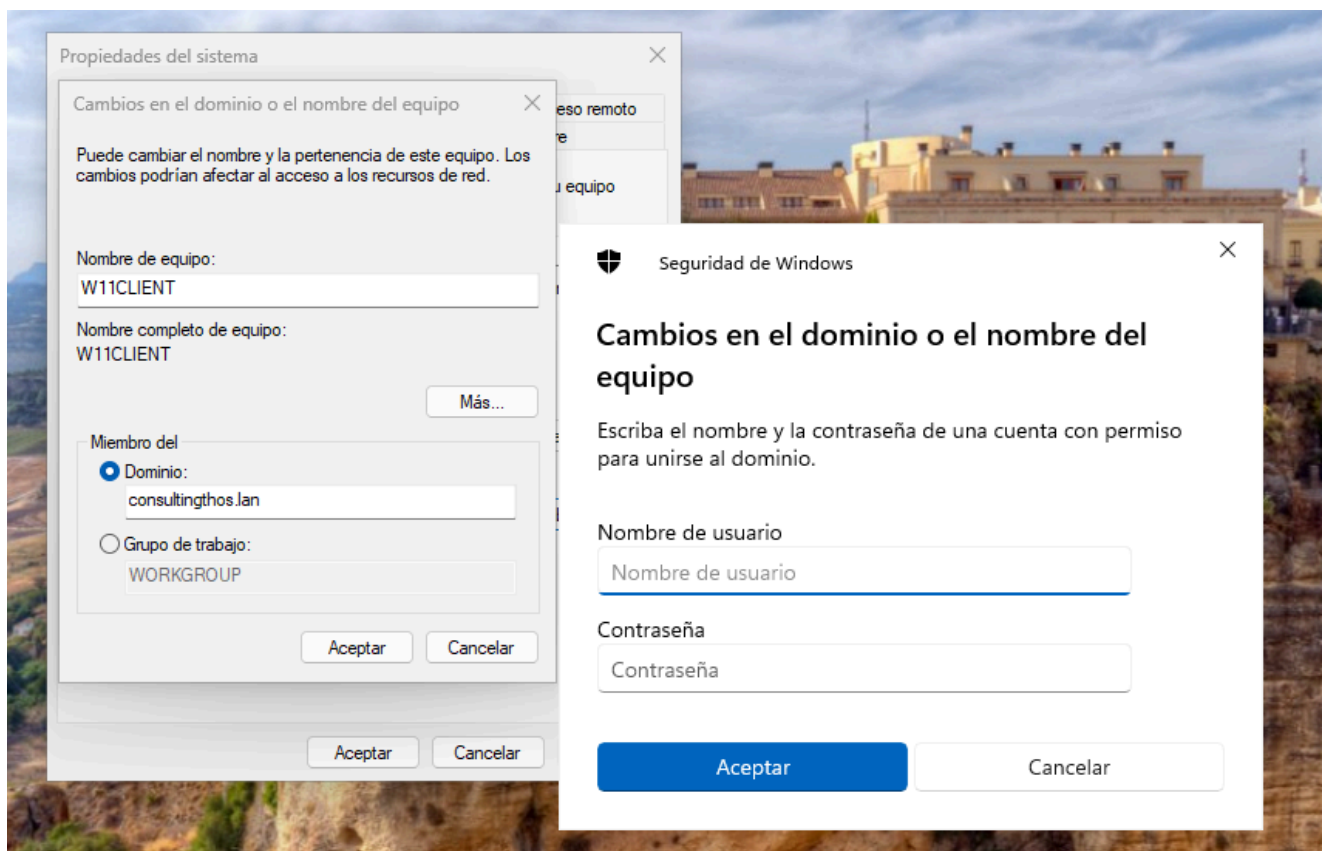
Si no tenemos ningún paquete perdido, podemos dar esta configuración por concluida.

Conexión al dominio

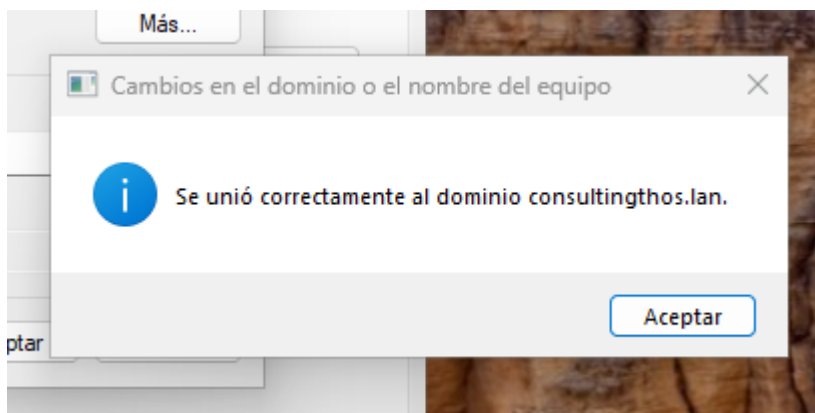
Para conectarse al dominio haremos lo siguiente:

```
Panel de control > (buscar)-Dominio > Unirse a dominio > Cambiar > Dominio-
(consultingthos.lan)
```

Si nos pide la configuración de administrador, la introducimos:



Una vez introducido, nos aparecerá la confirmación:

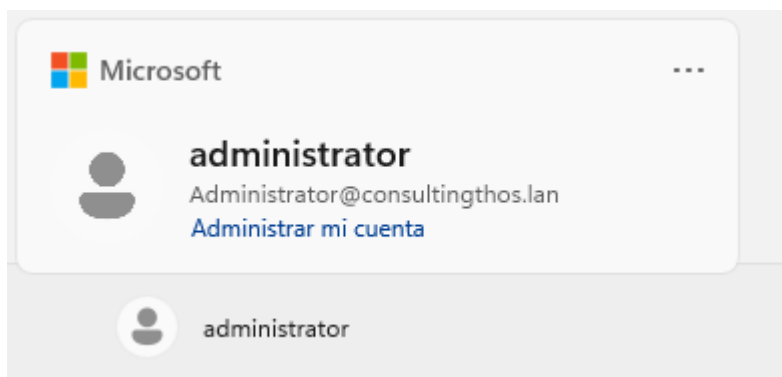


Deberemos reiniciar el equipo para que se realicen los cambios.

Una vez reiniciado, iniciamos como "administrator":

"ABAJO A LA IZQUIERDA" > Otro usuario >

```
usuario: administrator
password: -'CONFIDENCIAL' -
```



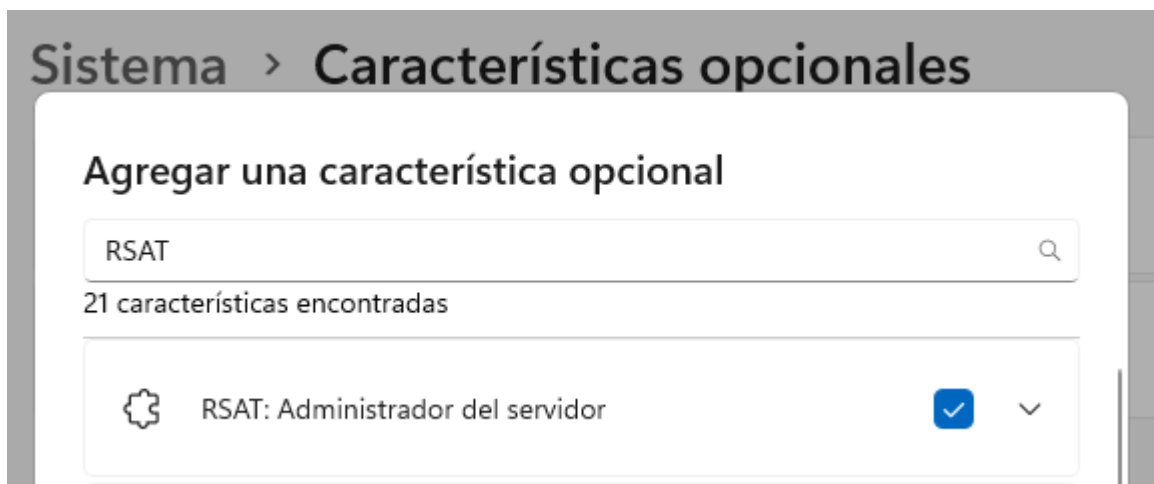
Posibles errores de conexión al dominio:

- Verifica que el DNS está apuntando al servidor (192.168.0.1/24)
- EN EL SERVIDOR → Verifica que las resoluciones DNS estén bien configuradas (tanto en el /etc/resolv.conf como en /etc/samba/smb.conf)

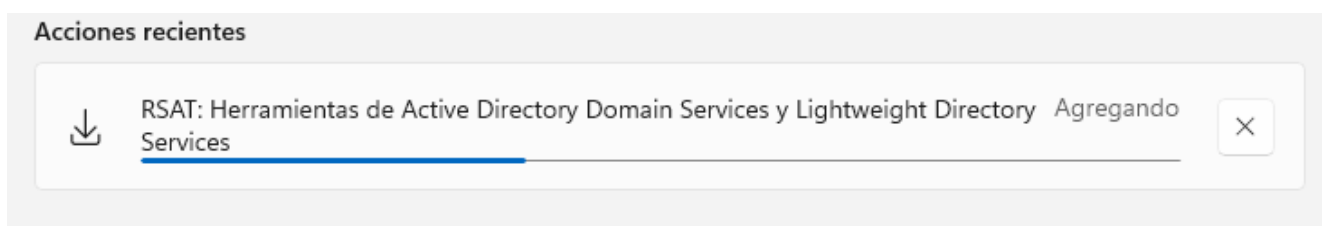
Instalación de las RSAT

Para instalar las RSAT, deberemos entrar a configuración y buscar "Características Opcionales"

Configuración > (buscar)-"Características opcionales" > Ver características > (buscar)-"RSAT"

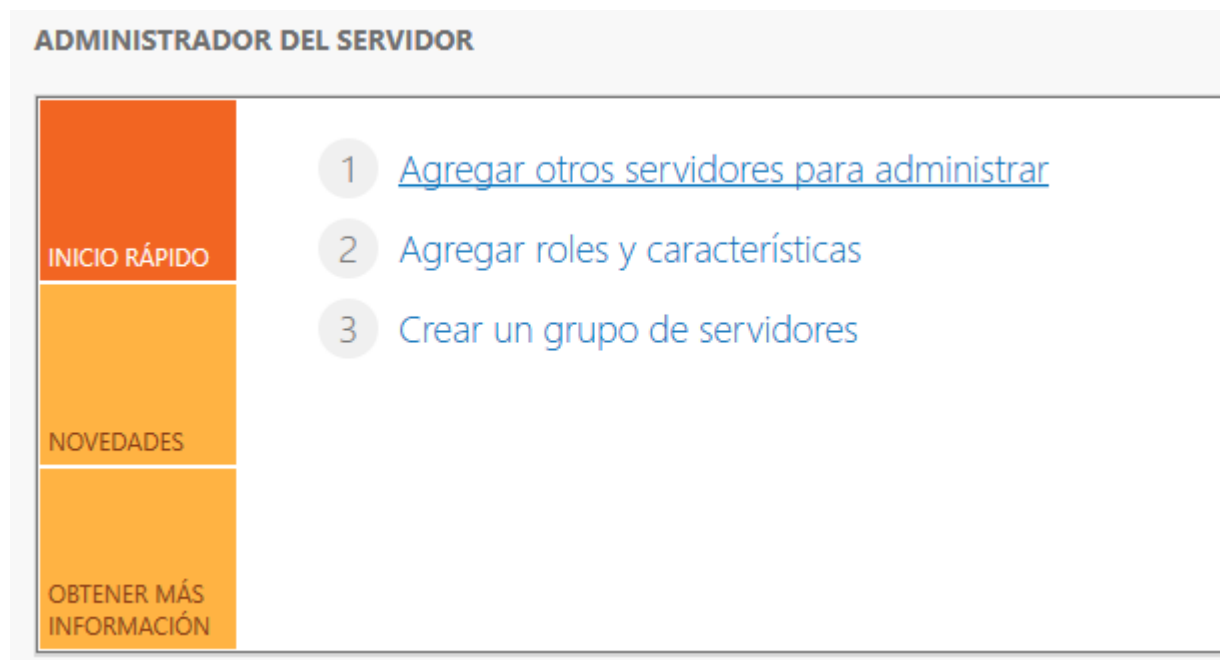


Le damos a instalar y esperamos

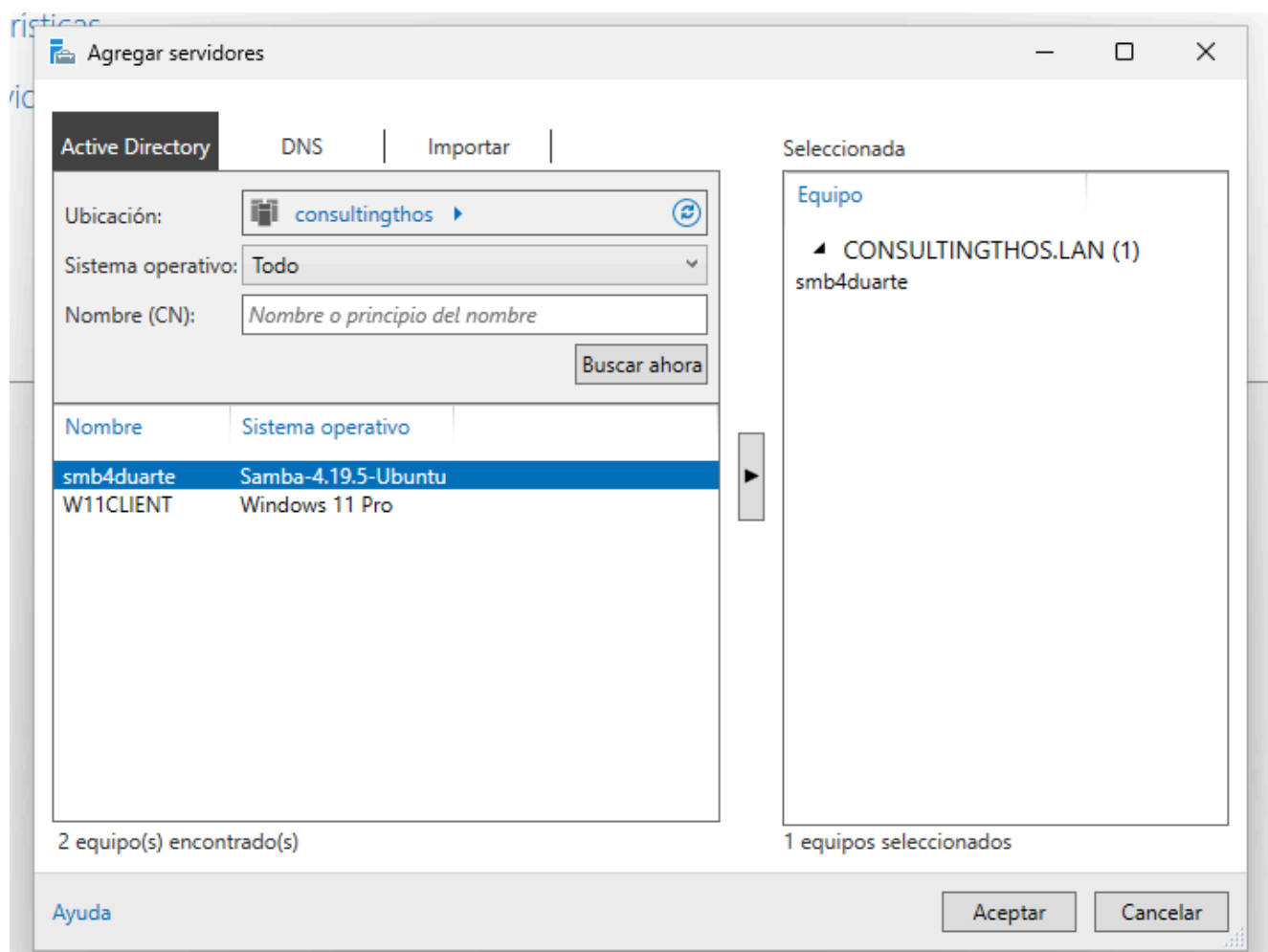


Selección del servidor para administrar

Abriremos la aplicación "Administrador del servidor" y seleccionaremos el primer apartado ("*Agregar otros servidores para administrar*")



Añadiremos el servidor samba (aparecerá con su hostname)

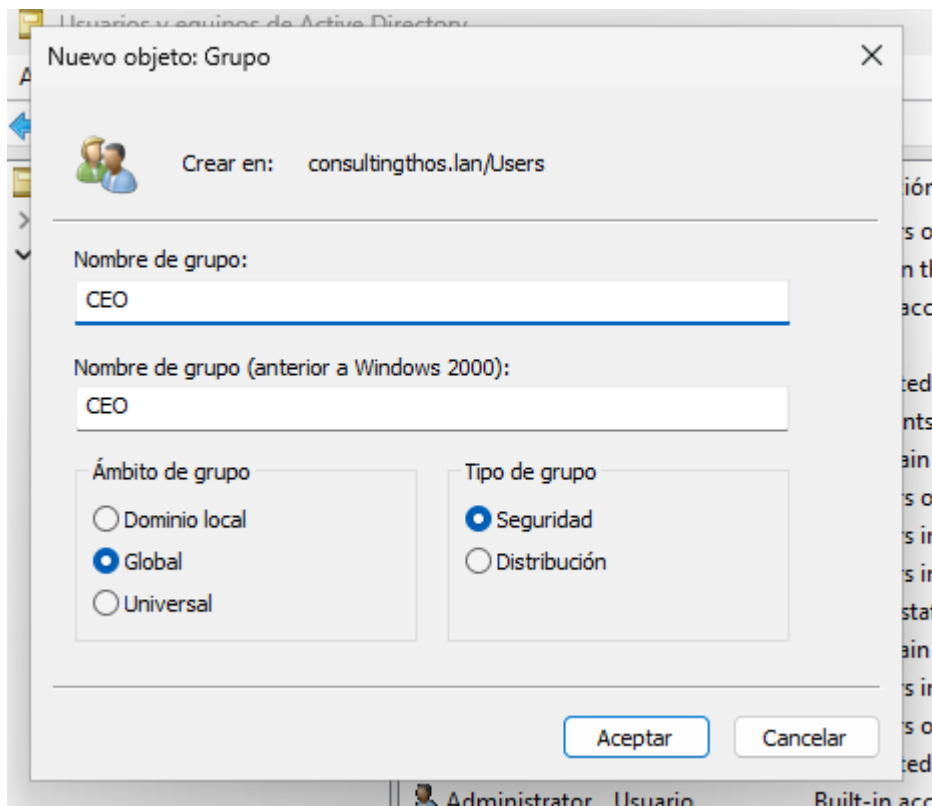


Le damos a aceptar.

Creación de un grupo de seguridad y un usuario

En este caso, crearemos al grupo CEO como grupo de seguridad y crearemos también al usuario Gerard Prat, el cual formará parte de ese grupo.

(buscar)-Usuarios y equipos de active directory > (clic derecho a consultingthos.lan)-nuevo > grupo > (nombre)-CEO



Ahora el usuario:

(Dentro de)-users > (clic derecho en cualquier lado)-Nuevo > usuario

Ponemos las siguientes credenciales:

Nombre de pila: Gerard

Iniciales: GP

Apellidos: Prat

--

Nombre de inicio de sesión del usuario:

gprat@consultingthos.lan

Nuevo objeto: Usuario

Crear en: consultingthos.lan/Users

Nombre de pila: Gerard Iniciales: GP

Apellidos: Prat

Nombre completo: Gerard GP. Prat

Nombre de inicio de sesión de usuario: gprat @consultingthos.lan

Nombre de inicio de sesión de usuario (anterior a Windows 2000): CONSULTINGTHOS\ gprat

< Atrás Siguiente > Cancelar

Haremos que su contraseña no caduque nunca:

Nuevo objeto: Usuario

Crear en: consultingthos.lan/Users

Cuando haga clic en Finalizar, se creará el siguiente objeto:

Nombre completo: Gerard GP. Prat

Nombre de inicio de sesión del usuario: gprat@consultingthos.lan

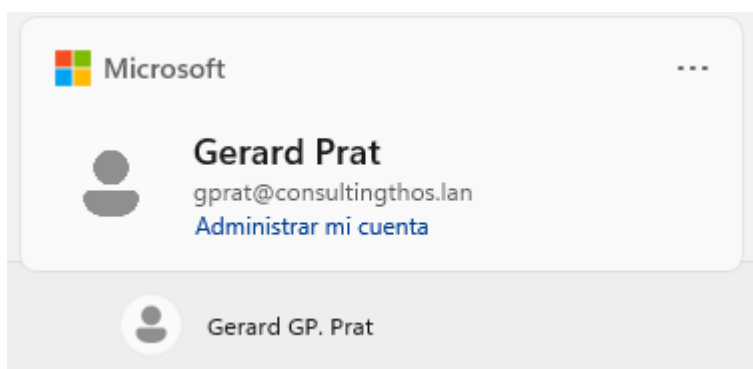
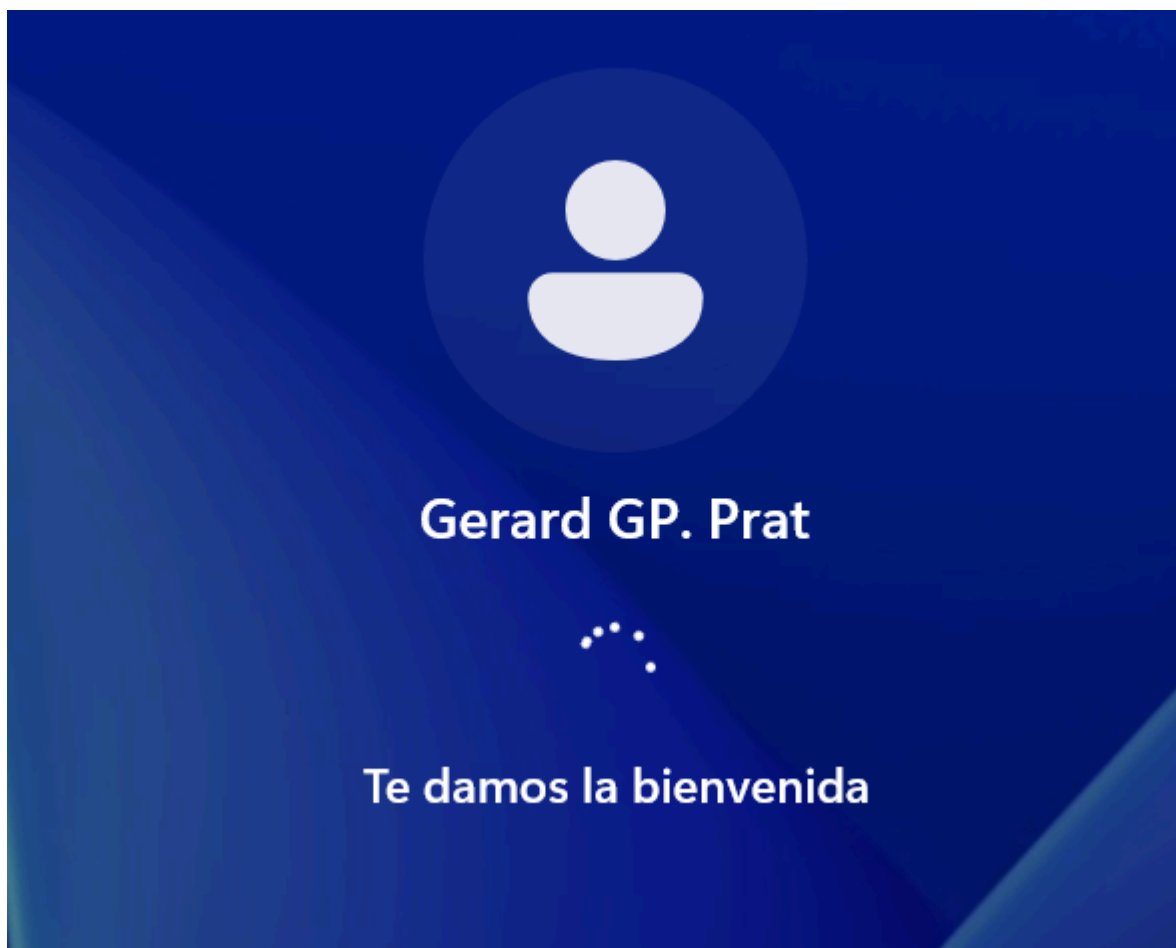
La contraseña nunca expira.

< Atrás Finalizar Cancelar

Cerraremos sesión (o reiniciar) e iniciaremos sesión como GPrat:

"ABAJO A LA IZQUIERDA" > Otro usuario >

```
usuario: gprat
password: -'CONFIDENCIAL' -
```



Verificación de visibilidad de la carpeta compartida

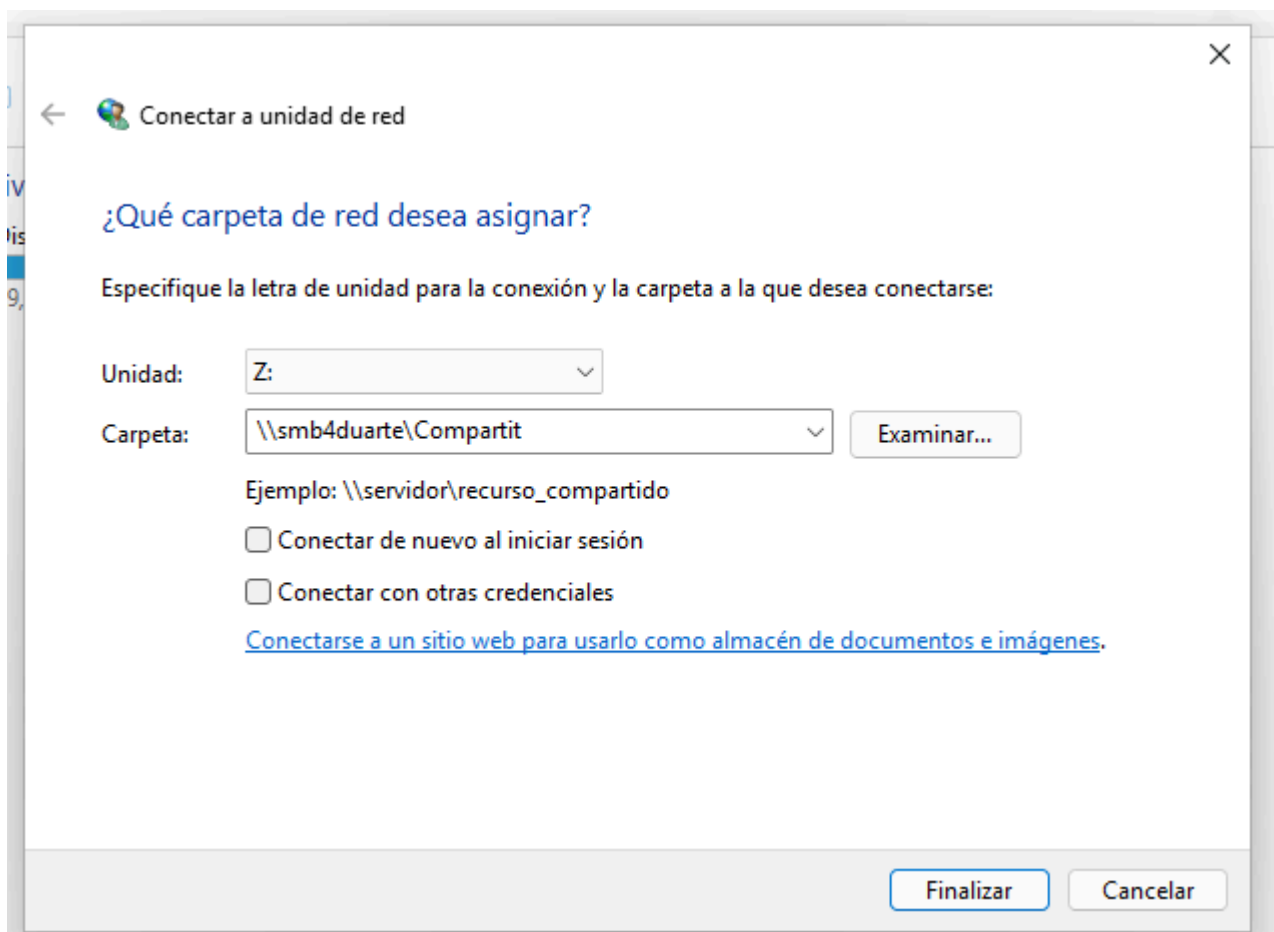
Antes, hemos generado una carpeta compartida en el fichero `smb.conf` en el servidor.
Verifiquemos a ver si es visible:

```
CTRL+E > (click derecho a "Este equipo")-Conectar unidad de red
```

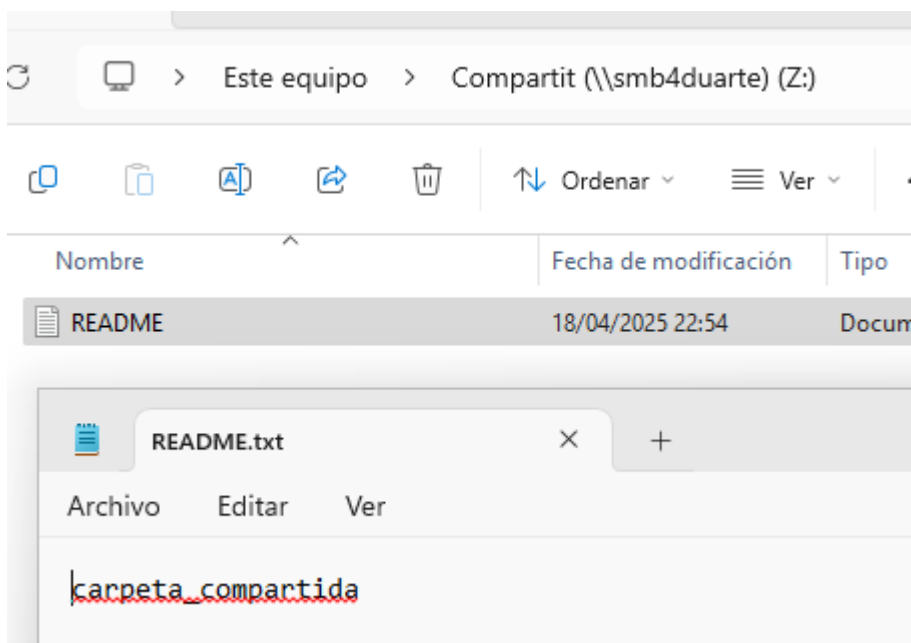
```
--
```

```
Unidad: Z:
```

```
Carpeta: \\smb4duarte\Compartit
```



Si le damos a finalizar, se nos abrirá automáticamente la unidad Z, y podremos ver el fichero **README.txt** que creamos cuando configuramos la carpeta compartida:

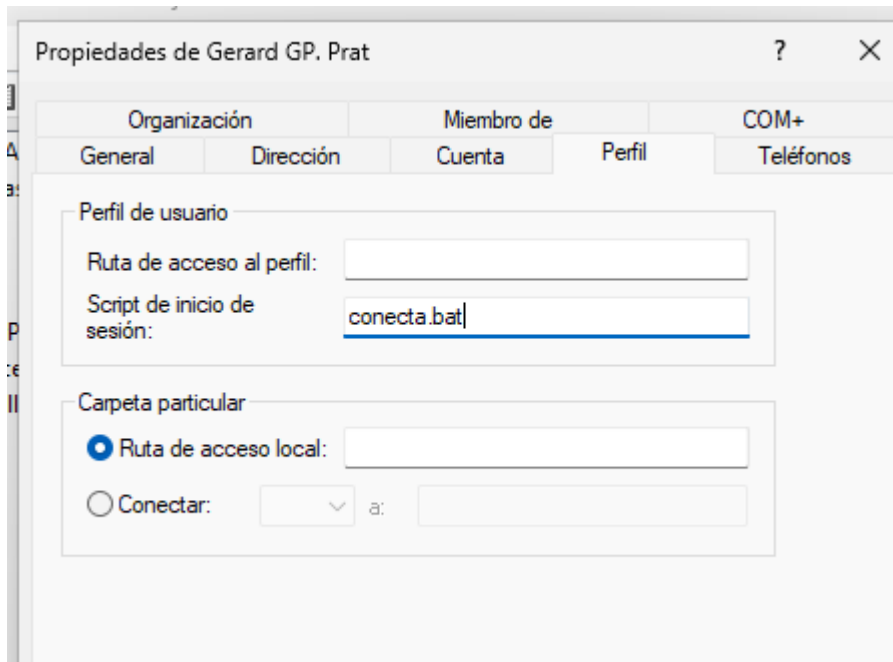


Configuración del script de inicio de sesión

Iniciamos sesión como ****_administrator_**** y iremos a:

```
Usuarios y equipos de active directory > users > (click derecho)-Gerard GP.  
Prats > Propiedades > Perfil
```

Script de inicio de sesión: conecta.bat



Aplicamos y reiniciamos. Luego iniciaremos sesión como Gprat.

Abrimos el Explorador de archivos y automáticamente, en la pestaña de "Este equipo" debería de haber conectado automáticamente en la unidad Z: la carpeta compartida:

