Tutoriales:
https://www.tecmint.com/manage-samba4-active-directory-linux-command-line/
https://www.tecmint.com/manage-samba4-ad-from-windows-via-rsat/

1) Se crea un usuario y se agrega al grupo de administradores del directorio:

- sudo samba-tool user add OperacionesAdmin
- sudo samba-tool group addmembers Administrators OperacionesAdmin

Se puede verificar si el usuario fue creado y si fue agregado al grupo correctamente con los respectivos comandos:

- sudo samba-tool user list | grep OperacionesAdmin
- sudo samba-tool group listmembers “Domain Admins”

2) Se configura la posibilidad de ingresar localmente a Linux con las cuentas disponibles en el Active Directory.

2.1) Se agrega lo siguiente al archivo smb.conf

- sudo nano /etc/samba/smb.conf

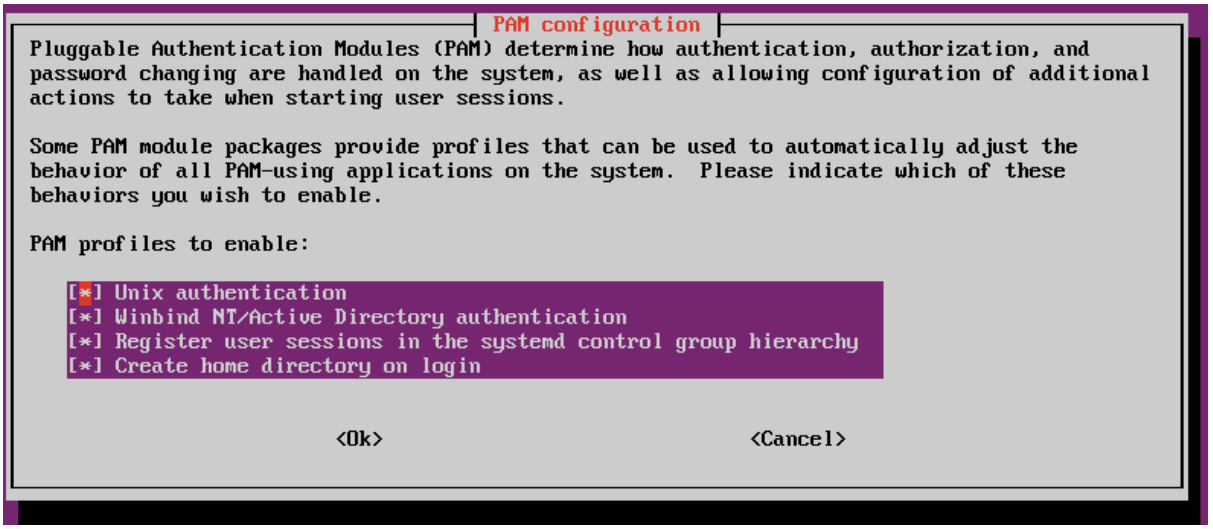
```
# Global parameters
[global]
        workgroup = OPERACIONES
        realm = OPERACIONES.LAN
        netbios name = SAMBA
        server role = active directory domain controller
        dns forwarder = 8.8.8.8
        idmap_ldb:use rfc2307 = yes

        template shell = /bin/bash
        winbind use default domain = true
        winbind offline logon = false
        winbind nss info = rfc2307

        winbind enum users = yes
        winbind enum groups = yes

[netlogon]
        path = /var/lib/samba/sysvol/operaciones.lan/scripts
        read only = No

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

2.2) Se verifica el estado del archivo y se reinicia el servicio respectivamente:

- testparm
- sudo systemctl restart samba-ad-dc.service

2.3) Se modifica la configuración PAM para permitir autenticación mediante AD:

- sudo pam-auth-update



2.4) Se modifica el archivo nsswitch.conf y se agrega “winbind” a passwd y group:

- sudo nano /etc/nsswitch.conf

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

2.5) Se modifica el archivo common-password, con el fin de permitir el cambio de contraseña desde la consola en linux:

- sudo nano /etc/pam.d/common-password
- remover “use_authtok” en la línea “password [success=1 default…”

```
# here are the per-package modules (the "Primary" block)
password        [success=2 default=ignore]      pam_unix.so obscure sha512
password        [success=1 default=ignore]      pam_winbind.so try_first_pass
```

3) Desactivar el servicio de winbind (Samba 4 trae uno integrado):

- sudo systemctl disable winbind.service
- sudo systemctl stop winbind.service

4) Instalar y configurar protocolo NTP, necesario para la sincronización entre AD y los usuarios:

- sudo apt-get install ntp ntpdate
- sudo nano /etc/ntp.conf

Se agregan servidores cercanos para NTP:

```
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
#pool 0.ubuntu.pool.ntp.org iburst
#pool 1.ubuntu.pool.ntp.org iburst
#pool 2.ubuntu.pool.ntp.org iburst
#pool 3.ubuntu.pool.ntp.org iburst

pool 0.south-america.pool.ntp.org
pool 1.south-america.pool.ntp.org
pool 2.south-america.pool.ntp.org

# Use Ubuntu's ntp server as a fallback.
pool 3.south-america.pool.ntp.org
```

Se agrega la línea “ntpsigndsocket …” en el mismo archivo:

```
driftfile /var/lib/ntp/ntp.drift
ntpsigndsocket /var/lib/samba/ntp_signd/
```

Se agrega la línea “restrict default kod…” en el mismo archivo:

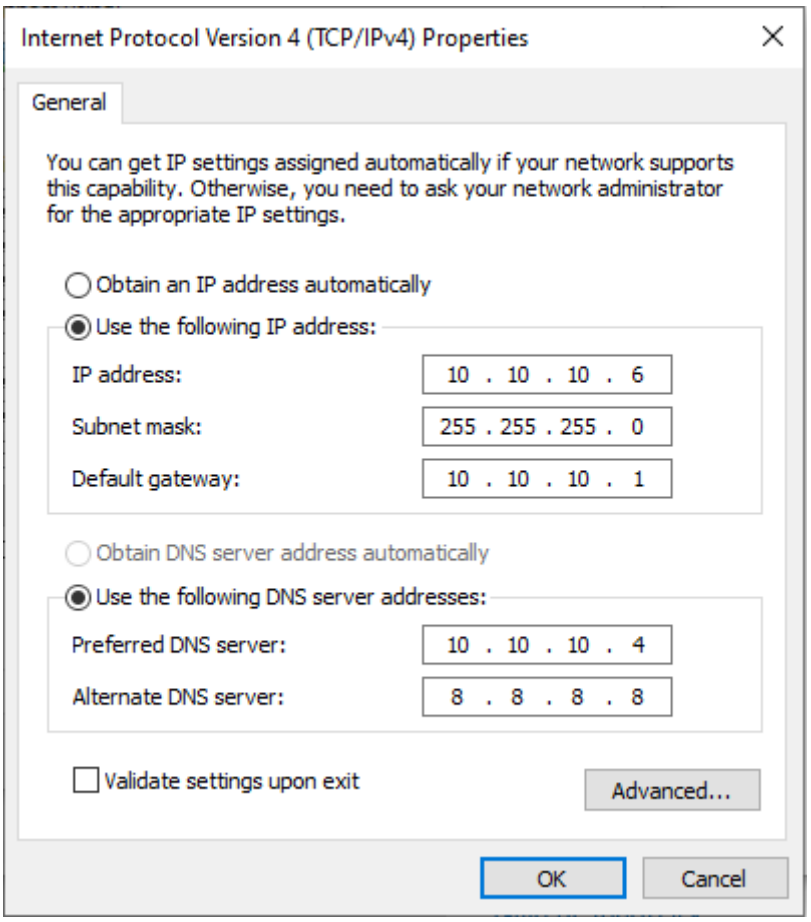
```
# Needed for adding pool entries
restrict source notrap nomodify noquery

restrict default kod nomodify notrap nopeer mssntp
```

Finalizar dando permiso a NTP para leer el directorio ntp_signd y reiniciando el servicio:

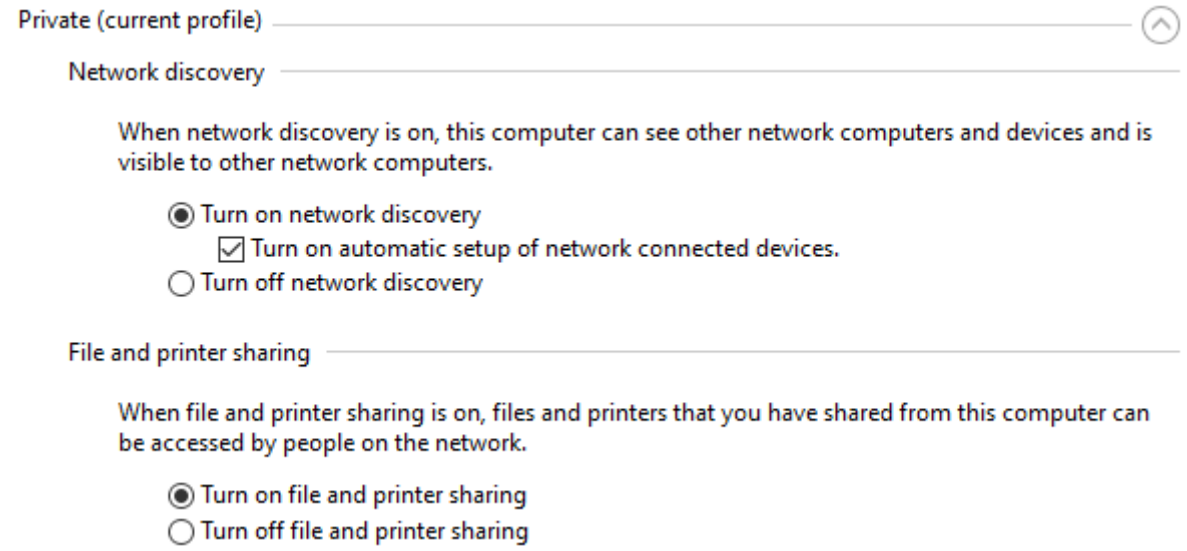
- sudo chown root:ntp /var/lib/samba/ntp_signd/
- sudo chmod 750 /var/lib/samba/ntp_signd/
- sudo systemctl restart ntp
- sudo netstat -tulpn | grep ntp

5) Agregar el usuario de Windows al directorio:

5.1) Se configura el cliente de Windows (Control panel, Network and Internet, Network and Sharing Center, Change adapter settings, Properties (del adaptador de red), Internet Protocol Version 4 (TCP/IPv4) Properties:



5.2) Configurar las preferencias para ser visto a través de la red (Control panel, Network and Internet, Network and Sharing Center, Change advanced sharing settings. Activar el network discovery tanto de forma privada como pública:



5.3) Se prueba la conexión desde el cliente hacia el servidor AD:

```
C:\Users\Roberto>ping operaciones.lan

Pinging operaciones.lan [10.10.10.4] with 32 bytes of data:
Reply from 10.10.10.4: bytes=32 time<1ms TTL=64
Reply from 10.10.10.4: bytes=32 time<1ms TTL=64
Reply from 10.10.10.4: bytes=32 time<1ms TTL=64
Reply from 10.10.10.4: bytes=32 time=1ms TTL=64

Ping statistics for 10.10.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

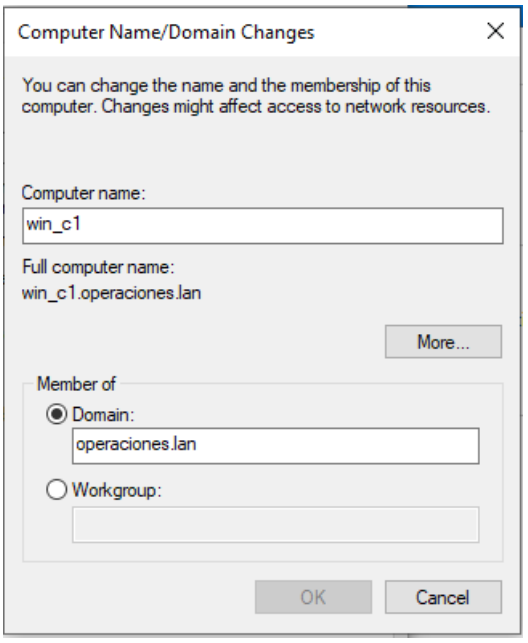
5.4) Se prueba la conexión desde el servidor AD hacia el cliente:

```
robert@samba:~$ ping -c3 10.10.10.6
PING 10.10.10.6 (10.10.10.6) 56(84) bytes of data.
64 bytes from 10.10.10.6: icmp_seq=1 ttl=128 time=0.294 ms
64 bytes from 10.10.10.6: icmp_seq=2 ttl=128 time=0.385 ms
64 bytes from 10.10.10.6: icmp_seq=3 ttl=128 time=0.221 ms

--- 10.10.10.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.221/0.300/0.385/0.067 ms
```

5.5) Configurar la sincronización de tiempo entre el cliente y el servidor (Control panel, Clock and Region, Set the time and date, Internet Time tab, Change settings):

- Activar la sincronización con un servidor de internet
- añadir operaciones.lan como el servidor
- Presionar “Update Now” (probablemente dos veces)

5.6) Añadir el cliente como un usuario del directorio (Control panel, System and security, System, Change settings, Botón “Change…”):



5.7) Para confirmar los cambios es necesario utilizar una cuenta administrador como la creada al inicio (OperacionesAdmin). Posteriormente reiniciar Windows y se podrá iniciar sesión mediante alguna cuenta creada en AD (nuevamente, OperacionesAdmin por ejemplo).

Posterior a esto es posible instalar las herramientas RSAT dentro de Windows y manejar la creación de usuarios y grupos desde estas sin necesidad de entrar al servidor de samba y utilizar samba-tool.