

Creación de el nuevo linux server.

Configurar el archivo:

```
sudo nano /etc/netplan/50-cloud-init.yaml
```

```
GNU nano 6.2                               /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 172.30.20.120/16
      routes:
        - to: default
          via: 172.30.20.1
      nameservers:
        addresses:
          - 10.239.3.7
          - 10.239.3.8
    enp0s8:
      addresses:
        - 192.168.10.120/24
```

network:

version: 2

renderer: networkd

ethernets:

enp0s3:

addresses:

- 172.30.20.120/16

routes:

- to: default

via: 172.30.20.1

nameservers:

addresses:

- 10.239.3.7

- 10.239.3.8

enp0s8:

addresses:

- 192.168.10.120/24

Reiniciar :

sudo netplan apply

Configurar el hostname y la IP fija.

sudo hostnamectl set-hostname ls204

Reiniciar

reboot

Instalar el SSH:

sudo apt install openssh-server

ssh sergio@172.30.20.120

Luego dentro de:

sudo nano /etc/hosts

```
GNU nano 6.2                                     /etc/hosts
127.0.0.1 localhost
127.0.1.1 ls2044
192.168.10.120 ls2044.lab2044.lan ls2044
# 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
```

Verificar haciendo ping al nombre ls204 automáticamente tengo respuesta.

```
sergio@ls204:~$ ping ls204
PING ls204 (127.0.1.1) 56(84) bytes of data.
64 bytes from ls204 (127.0.1.1): icmp_seq=1 ttl=64 time=0.036 ms
64 bytes from ls204 (127.0.1.1): icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from ls204 (127.0.1.1): icmp_seq=3 ttl=64 time=0.038 ms
^C
--- ls204 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.033/0.035/0.038/0.002 ms
sergio@ls204:~$ ^C
sergio@ls204:~$
```

Antes debo deshabilitar el archivo resolved

sudo systemctl disable --now systemd-resolved

Es donde apunta a mi servidor para resolver los nombres de dominios ya que voy a implementar el servidor samba por que es incompatible.

Lo siguiente es eliminar el enlace simbólico las modificaciones que se hagan en este ya no se hagan si no en el verdadero.

sudo unlink /etc/resolv.conf

Crear un nuevo fichero resolv.conf

sudo nano /etc/resolv.conf

```
GNU nano 7.2                                     /etc/resolv.conf *
nameserver 192.168.10.15
nameserver 10.239.3.7
search lab15.lan
```

sudo chattr +i /etc/resolv.conf

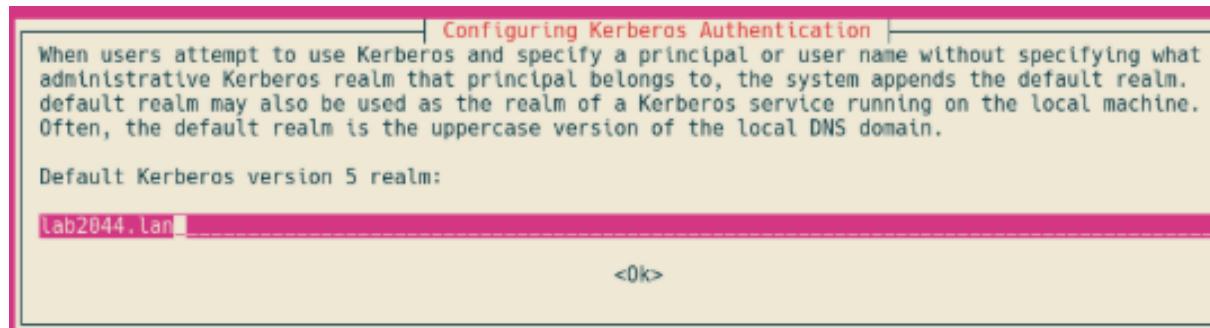
Con los siguientes comandos instalar samba:

sudo apt update

```
sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules
smbclient winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user
dnsutils chrony net-tools
```

Durante la instalación pedirá el dominio de servidores para kerberos, poner el dominio:

lab2044.lan



ls2044.lab2044.lan



ls2044.lab2044.lan



Deshabilitar servicios Samba clásicos

Detener y deshabilitar los servicios que Active Directory que no se van a usar.

sudo systemctl stop smbd nmbd winbind

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

```
sergio@ls2044:~$ sudo systemctl stop smbd nmbd winbind
sergio@ls2044:~$ sudo systemctl disable smbd nmbd winbind
Synchronizing state of smbd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable smbd
Synchronizing state of nmbd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable nmbd
Synchronizing state of winbind.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable winbind
Removed /etc/systemd/system/multi-user.target.wants/winbind.service.
Removed /etc/systemd/system/multi-user.target.wants/nmbd.service.
Removed /etc/systemd/system/multi-user.target.wants/smbd.service.
sergio@ls2044:~$
```

El servidor solo necesita samba ad-dc para funcionar como Active Directory:

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

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

Crear una copia de seguridad del archivo:

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

Provisionar el AD Samba:

Ejecutar provisionado:

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

```
sergio@ls2044:~$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
sergio@ls2044:~$ sudo samba-tool domain provision
Realm: lab2044.lan
Domain [lab2044]:
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) [192.168.10.128]: 10.239.3.7
```

dns es 10.239.3.7

Crear copia de seguridad de la configuración predeterminada de kerberos:

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

Reemplazar con el archivo /var/lib/samba/krb5.conf:

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

No edite nada lo deje porque ya estaba configurado :

sudo nano /etc/krb5.conf

Activar el controlador de dominio:

Iniciar servicio samba Active Directory samba-ad-dc:

sudo systemctl start samba-ad-dc

Comprobar servicios:

sudo systemctl status samba-ad-dc

```
● samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/lib/systemd/system/samba-ad-dc.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2026-02-02 09:29:45 UTC; 10s ago
     Docs: man:samba(8)
           man:samba(7)
           man:smb.conf(5)
 Main PID: 5146 (samba)
   Status: "samba: ready to serve connections..."
    Tasks: 60 (limit: 2219)
   Memory: 203.3M
      CPU: 3.125s
 CGroup: /system.slice/samba-ad-dc.service
         ├─5146 "samba: root process" " "
         ├─5147 "samba: tfork waiter process(5148)" " "
         ├─5148 "samba: task[s3fs] pre-fork master" " "
         ├─5149 "samba: tfork waiter process(5150)" " "
         ├─5150 "samba: task[rpc] pre-fork master" " "
         ├─5151 "samba: tfork waiter process(5153)" " "
         ├─5152 "samba: tfork waiter process(5156)" " "
         ├─5153 "samba: task[nbt] pre-fork master" " "
         ├─5154 "samba: tfork waiter process(5157)" " "
         ├─5155 "samba: tfork waiter process(5159)" " "
         ├─5156 /usr/sbin/smbd -D "--option=server role check:inhibit=yes" --foreground ""
         ├─5157 "samba: task[wrepl] pre-fork master" " "
         ├─5158 "samba: tfork waiter process(5161)" " "
         ├─5159 "samba: task[rpc] pre-forked worker(0)" " "
         ├─5160 "samba: tfork waiter process(5163)" " "
         ├─5161 "samba: task[ldap] pre-fork master" " "

```

Lines 1-28

Cambiar el permiso y la propiedad predeterminados del directorio
`/var/lib/samba/ntp_signd`:

sudo chown root:_chrony /var/lib/samba/ntp_signd

```
sergio@ls04:~$ sudo chown root:_chrony /var/lib/samba/ntp_signd
```

sudo chmod 750 /var/lib/samba/ntp_signd

```
sergio@ls04:~$ sudo chmod 750 /var/lib/samba/ntp_signd
sergio@ls04:~$
```

Modificar el archivo de configuración /etc/chrony/chrony.conf:

sudo nano /etc/chrony/chrony.conf

Al final de todo agregar esto:

```
bindcmdaddress 192.168.10.37
allow 192.168.10.0/24
ntpsigndsocket /var/lib/samba/ntp_signd
```

```
# Get TAI-UTC offset and leap seconds from the system tz database.
# This directive must be commented out when using time sources serving
# leap-smeared time.
leapsectz right/UTC
bindcmdaddress 192.168.10.37
allow 192.168.10.1
ntpsigndsocket /var/lib/samba/ntp_signd
```

Reiniciar chrony:

sudo systemctl restart chronyd

Verificar:

sudo systemctl status chronyd

Verificar nombres de dominio

```
host -t A lab04.lan
host -t A ls04.lab04.lan
```

```
sergio@ls04:~$ sudo systemctl start samba-ad-dc
sergio@ls04:~$ host -t A LAB04.LAN
LAB04.LAN has address 172.30.20.39
LAB04.LAN has address 192.168.10.37
sergio@ls04:~$ sudo nano /etc/resolv.conf
sergio@ls04:~$ host -t A ls04.lab04.lan
ls04.lab04.lan has address 172.30.20.39
ls04.lab04.lan has address 192.168.10.37
sergio@ls04:~$ █
```

Verificar que los registros de servicios kerberos y ldap apunten al FQDN:

```
host -t SRV _kerberos._udp.lab04.lan
host -t SRV _ldap._tcp.lab04.lan
```

```
ls04.lab04.lan has address 192.168.10.37
sergio@ls04:~$ host -t SRV _kerberos._udp.lab04.lan
_kerberos._udp.lab04.lan has SRV record 0 100 88 ls04.lab04.lan.
sergio@ls04:~$ host -t SRV _ldap._tcp.lab04.lan
_ldap._tcp.lab04.lan has SRV record 0 100 389 ls04.lab04.lan.
sergio@ls04:~$ █
```

Verificar que los recursos predeterminados están disponibles en Samba Active Directory:

```
smbclient -L lab04.lan -N
```

```
_tcp._tcp.lab04.lan has SRV record 0 100 389 ls04.lab04.lan.
sergio@ls04:~$ smbclient -L lab04.lan -N
Anonymous login successful

      Sharename      Type      Comment
      -----      ----      -----
      sysvol        Disk
      netlogon       Disk
      IPC$          IPC       IPC Service (Samba 4.19.5-Ubuntu)
SMB1 disabled -- no workgroup available
sergio@ls04:~$ █
```

Validación Final:

Comprobar autenticación en el servidor de kerberos mediante el administrador:

kinit administrator@LAB2044.LAN

```
sergio@ls2044:~$ kinit administrator@LAB2044.LAN
Password for administrator@LAB2044.LAN:
Warning: Your password will expire in 41 days on Mon Mar 16 09:29:02 2024
sergio@ls2044:~$ █
```

klist

```
sergio@ls2044:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@LAB2044.LAN

Valid starting     Expires            Service principal
02/02/26 09:45:11  02/02/26 19:45:11  krbtgt/LAB2044.LAN@LAB2044.LAN
    renew until 02/03/26 09:45:06
sergio@ls2044:~$ █
```

Cliente Linux

Configurar nombre del equipo:

sudo hostnamectl set-hostname lc04

Configurar red del equipo:

Ahora hay que configurar el la red como lo pone en la imagenes y recuerda en (IPV4) .



Ahora comprobamos haciendo un ping:

Cliente:

```
sergio@lc04:~$ ping -c 2 192.168.10.37
PING 192.168.10.37 (192.168.10.37) 56(84) bytes of data.
64 bytes from 192.168.10.37: icmp_seq=1 ttl=64 time=0.292 ms
64 bytes from 192.168.10.37: icmp_seq=2 ttl=64 time=0.314 ms

--- 192.168.10.37 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1042ms
rtt min/avg/max/mdev = 0.292/0.303/0.314/0.011 ms
sergio@lc04:~$
```

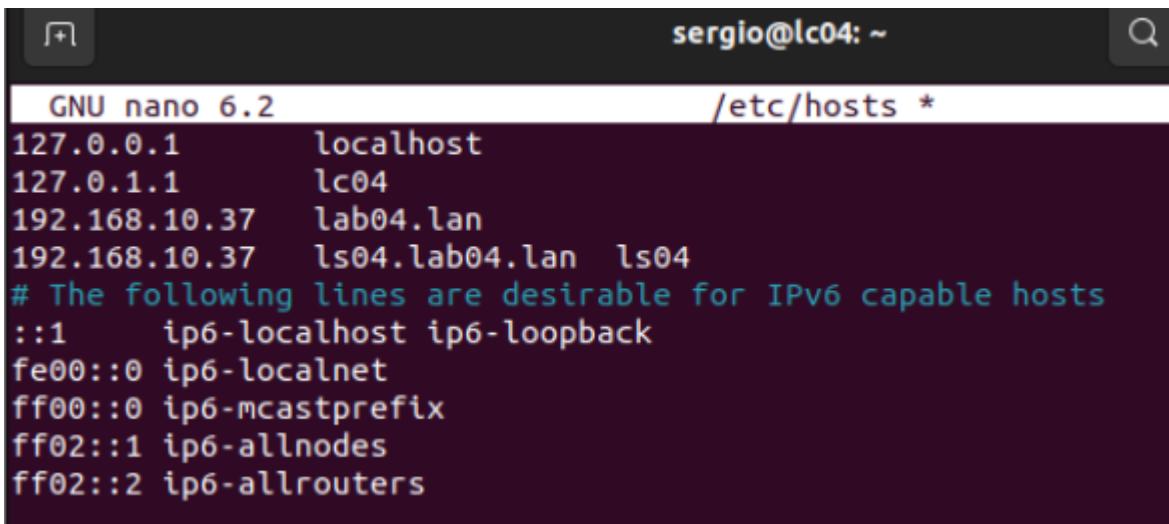
Server:

```
sergio@ls04: ~$ 
sergio@ls04:~$ ping -c 2 192.168.10.38
PING 192.168.10.38 (192.168.10.38) 56(84) bytes of data.
64 bytes from 192.168.10.38: icmp_seq=1 ttl=64 time=0.435 ms
64 bytes from 192.168.10.38: icmp_seq=2 ttl=64 time=0.291 ms

--- 192.168.10.38 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.291/0.363/0.435/0.072 ms
sergio@ls04:~$ _
```

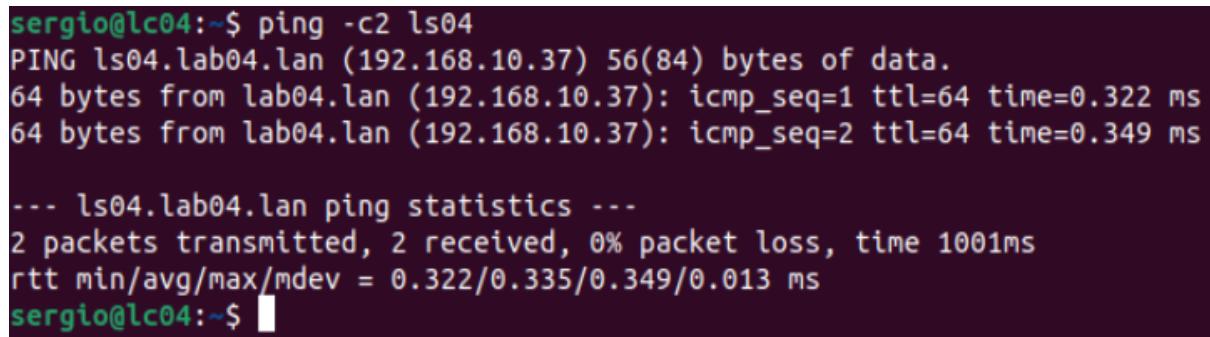
Ahora configuramos el archivo:

sudo nano /etc/hosts



```
GNU nano 6.2          /etc/hosts *
127.0.0.1      localhost
127.0.1.1      lc04
192.168.10.37   lab04.lan
192.168.10.37   ls04.lab04.lan  ls04
# 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
```

Comprobación:



```
sergio@lc04:~$ ping -c2 ls04
PING ls04.lab04.lan (192.168.10.37) 56(84) bytes of data.
64 bytes from lab04.lan (192.168.10.37): icmp_seq=1 ttl=64 time=0.322 ms
64 bytes from lab04.lan (192.168.10.37): icmp_seq=2 ttl=64 time=0.349 ms

--- ls04.lab04.lan ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.322/0.335/0.349/0.013 ms
sergio@lc04:~$
```

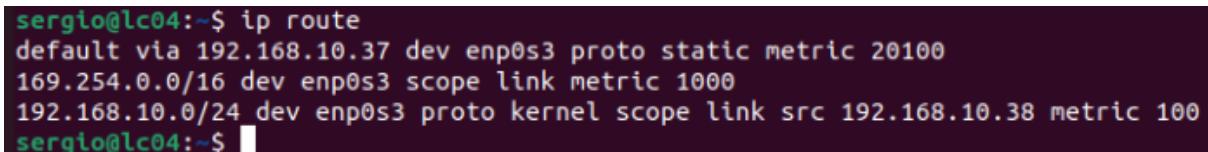
Ahora toca la configuración de netplan :

-Primero poner en modo root.

sudo su

Después comprobar siguiente:

ip route



```
sergio@lc04:~$ ip route
default via 192.168.10.37 dev enp0s3 proto static metric 20100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.10.0/24 dev enp0s3 proto kernel scope link src 192.168.10.38 metric 100
sergio@lc04:~$
```

Verificar haciendo ping al servidor con IP, DNS y conexión a internet.

-Si aún no hay conexión a internet ver estas configuraciones.

Verifica que el servidor tenga activado el reenvío IP:

sudo nano /etc/sysctl.conf

Añadir al final :

net.ipv4.ip_forward=1

Aplicar y comprobar :

sudo sysctl -p

sysctl net.ipv4.ip_forward

```
sergio@ls04:~$ sudo sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
sergio@ls04:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
sergio@ls04:~$ sudo sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
sergio@ls04:~$
```

Configurar NAT correctamente en el servidor:

sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

Comprobar :

sudo iptables -t nat -L -n -v

```
sergio@ls04:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
sergio@ls04:~$ sudo iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source          destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source          destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source          destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source          destination
      22   1595 MASQUERADE  0    -- *      enp0s3  0.0.0.0/0           0.0.0.0/0
sergio@ls04:~$
```

Comprueba internet en el cliente.

Instalación del paquete **NTPDATE (en el cliente) y estar en root > sudo su**

sudo apt update

sudo apt-get install ntpdate

Esto sirve para sincronizar los relojes de las máquinas y puedan unirse al dominio sincronizados

Comprobar con:

sudo ntpdate -q lab04.lan

esto significa que hay una diferencia de -0.010688 segundos, con el siguiente comando voy a sincronizar >

sudo ntpdate lab15.lan

Instalar paquetes necesarios en Ubuntu Desktop:

sudo apt update

sudo apt-get install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind

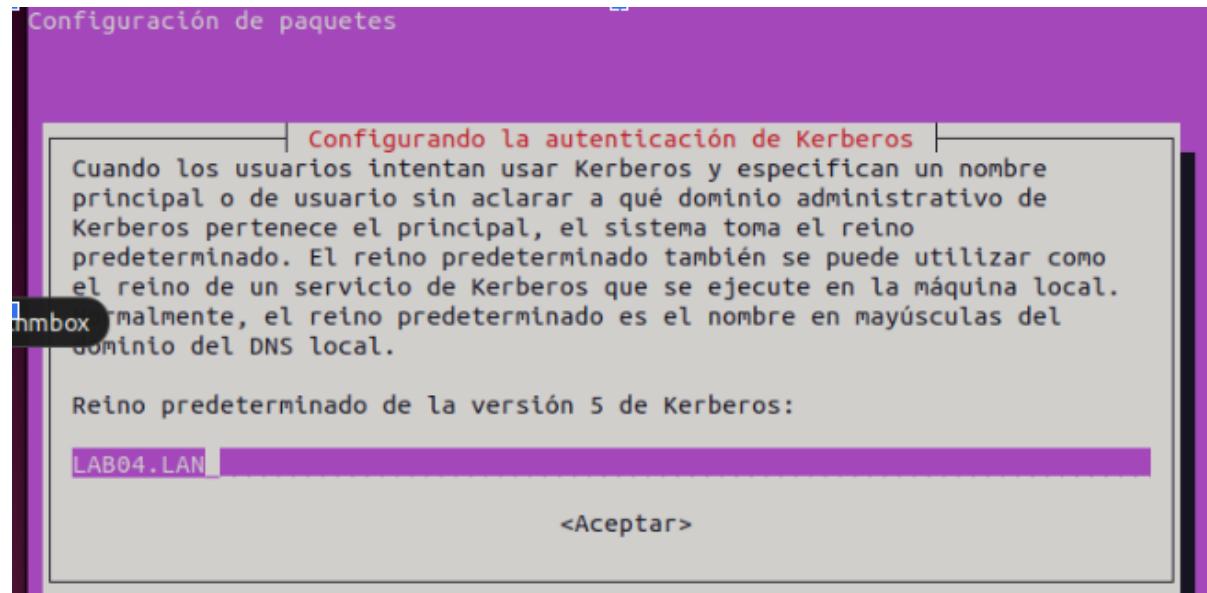
Si te da fallo usa esto:

sudo systemctl stop unattended-upgrades

sudo kill -9 4363

sudo dpkg --configure -a

```
sudo apt-get install samba krb5-config krb5-user winbind libpam-winbind  
libnss-winbind
```



```
kinit administrator@LAB04.LAN
```

```
klist
```

```
sergio@lc04:~$ kinit administrator@LAB04.LAN  
Password for administrator@LAB04.LAN:  
Warning: Your password will expire in 3 days on lun 12 ene 2026 13:15:50  
sergio@lc04:~$ klist  
Ticket cache: FILE:/tmp/krb5cc_1000  
Default principal: administrator@LAB04.LAN  
  
Valid starting     Expires            Service principal  
 09/01/26 09:05:03  09/01/26 19:05:03  krbtgt/LAB04.LAN@LAB04.LAN  
                  renew until 10/01/26 09:04:56
```

Mover archivo smb.conf y crear copia de seguridad.

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

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

```
GNU nano 6.2                               /etc/samba/smb.conf
[global]
    workgroup = LAB04
    realm = LAB04.LAN
    netbios name = lc04
    security = ADS
    dns forwarder = 192.168.10.37

    idmap config * : backend =t ldb
    idmap config *:range =50000-1000000

        template homedir = /home/%D/%U
        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

        vfs objects = acl_xattr
        map acl inherit = yes
        store dos attributes = yes
```

Agregar lo siguiente en el nuevo:

```
[global]
    workgroup = LAB15
    realm = LAB15.LAN
    netbios name = lc15
    security = ADS
    dns forwarder = 192.168.10.15

    idmap config * : backend = tdb
    idmap config *:range = 50000-1000000

        template homedir = /home/%D/%U
        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

        vfs objects = acl_xattr
        map acl inherit = Yes
        store dos attributes = Yes
```

Reiniciar los demonios de samba:

sudo systemctl restart smbd nmbd

Detener los servicios que no son necesarios dentro de ubuntu desktop, porque el cliente no va ser un controlador de dominio:

sudo systemctl stop samba-ad-dc

Lo siguiente es habilitar los servicios de samba que se van a necesitar con:

sudo systemctl enable smbd nmbd

```
sergio@lc04:~$ sudo systemctl enable smbd nmbd
Synchronizing state of smbd.service with SysV service script with /lib/systemd/systemd-
-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable smbd
Synchronizing state of nmbd.service with SysV service script with /lib/systemd/systemd-
-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nmbd
sergio@lc04:~$
```

Unir Ubuntu desktop a SAMBA AD DC:

Con el siguiente comando uniré el ubuntu desktop a mi dominio LAB04.LAN

sudo net ads join -U administrator

```
sergio@lc04:~$ sudo net ads join -U administrator
Password for [LAB04\administrator]:
Using short domain name -- LAB04
Joined 'LC04' to dns domain 'lab04.lan'
No DNS domain configured for lc04. Unable to perform DNS Update.
DNS update failed: NT_STATUS_INVALID_PARAMETER
sergio@lc04:~$
```

Servidor:

Entrar como root:

sudo su

ejecutar este comando:

sudo samba-tool computer list

```
sergio@ls04:~$ sudo su
[sudo] password for sergio:
root@ls04:/home/sergio# sudo samba-tool computer list
LS04$
LC04$
root@ls04:/home/sergio# _
```

CONFIGURAR AUTENTICACIÓN DE CUENTAS AD (cliente)

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 winbind
gshadow:     files

hosts:        files dns
networks:    files

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

netgroup:    nis
```

Si quieres que esté más actualizado pon file

```
passwd:      files winbind
group:       files winbind
shadow:      files winbind
hosts:        files dns
```

(cambiar a files winbind) PRUEBA

Reiniciar :

sudo systemctl restart winbind

Listar usuarios y grupos del dominio:

wbinfo -u y wbinfo -g

```
sergio@lc04:~$ wbinfo -u
administrator
guest
krbtgt
sergio@lc04:~$ wbinfo -g
schema admins
dnsupdateproxy
domain computers
Office Writer admins
enterprise read-only domain controllers
domain admins
protected users
domain guests
group policy creator owners
cert publishers
allowed rodc password replication group
ras and ias servers
dnsadmins
read-only domain controllers
domain controllers
denied rodc password replication group
domain users
sergio@lc04:~$
```

No hace falta

Verificar el módulo de winbind para tener el usuario administrator dentro de del equipo

sudo getent passwd | grep administrator

id administrator > muestra la información del usuario administrador, por lo tanto acceder con el usuario administrador

Configurar pam-auth-update para autenticarnos con cuentas de dominio y que se creen automáticamente los directorios.

sudo pam-auth-update

Marcar la opción de: Create home directory on login

Configuración de paquetes

Configuración de PAM

Los «Pluggable Authentication Modules» (PAM, o Módulos de autenticación insertables, N. del T.) determinan cómo se gestiona dentro del sistema la autenticación, autorización y modificación de contraseñas. También permiten la definición de acciones adicionales a realizar cuando se inicia la sesión de un usuario.

Algunos de los paquetes de módulos de PAM ofrecen perfiles que pueden utilizarse para ajustar automáticamente el comportamiento de todas las aplicaciones que utilicen PAM en el sistema. Indique qué comportamiento desea activar.

Perfiles PAM a habilitar:

- [*] Winbind NT/Active Directory authentication
- [*] SSS authentication
- [*] Register user sessions in the systemd control group hierarchy
- [*] Create home directory on login
- [*] GNOME Keyring Daemon - Login keyring management
- [*] Inheritable Capabilities Management

<Aceptar>

<Cancelar>

Editar el archivo para crear automáticamente los directorios cuando me logue:

sudo nano /etc/pam.d/common-account

Agregar al final de todo la siguiente línea

session required pam_mkhomedir.so skel=/etc/skel/ umask=0022

Agregar al final de todo la siguiente línea:

```
account [default=bad success=ok user_unknown=ignore]      pam_sss.so
# end of pam-auth-update config
session    required    pam_mkhomedir.so    skel=/etc/skel    umask=0022
```

Autenticarse con cuenta de usuario samba4 AD

Ingreso con usuario administrator y como está en la imagen he ingresado con el usuario administrator desde cli-ssd(ubuntu desktop)

El administrador no podrá usar sudo porque no está en el grupo sudoers para tener privilegios

en el root de la máquina usar este comando:

sudo usermod -aG sudo administrator

```
sergio@lc04:~$ sudo pam-auth-update
sergio@lc04:~$ sudo nano /etc/pam.d/common-account
sergio@lc04:~$ sudo su
root@lc04:/home/sergio# cd
root@lc04:~# sudo usermod -aG sudo administrator
root@lc04:~# su administrator
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Ahora si quiero loguearme con el usuario administrator del servidor ubuntu con interfaz gráfica cierro la sesión y entró con

administrator@lab04.lan

ingresar la contraseña y ya estare logueado con el usuario administrador desde ubuntu desktop



GESTIÓN DE USUARIOS Y GRUPOS EN SAMBA ACTIVE DIRECTORY y GPO

Desde el servidor Samba crear los grupos con su ámbito y usuarios:

```
sudo samba-tool group add IT_departments --group-scope=Universal
--group-type=Security
```

el scope puede ser: global, domain

```
sergio@ls04:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
[sudo] password for sergio:
sergio@ls04:~$ sudo iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in     out      source          destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in     out      source          destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in     out      source          destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in     out      source          destination
      3    216 MASQUERADE  0  -- *      enp0s3  0.0.0.0/0      0.0.0.0/0
sergio@ls04:~$ sudo samba-tool group add IT_departaments --group-scope=Universal --group-type=Security
Added group IT_departaments
sergio@ls04:~$ sudo samba-tool group add IT_admins --group-scope=Universal --group-type=Security
Added group IT_admins
sergio@ls04:~$ sudo samba-tool group add Students --group-scope=Universal --group-type=Security
Added group Students
sergio@ls04:~$ █
```

Crear los usuarios:

sudo samba-tool user create alice

```
sergio@ls04:~$ sudo samba-tool user create alice
[sudo] password for sergio:
New Password:
Retype Password:
User 'alice' added successfully
sergio@ls04:~$ █
```

Añadir los usuarios a los grupos correspondientes:

sudo samba-tool group addmembers IT_admins Alice

```
sergio@ls04:~$ sudo samba-tool group addmembers Students charlie
Added members to group Students
sergio@ls04:~$ sudo samba-tool group addmembers Students bob
Added members to group Students
sergio@ls04:~$ █
```

Crear Unidades Organizativas:

sudo samba-tool ou create "OU=IT_departaments,DC=lab04,DC=lan"

```
sergio@ls04:~$ sudo samba-tool ou create "OU=IT_departaments,DC=lab04,DC=lan"
Added ou "OU=IT_departaments,DC=lab04,DC=lan"
sergio@ls04:~$ sudo samba-tool ou create "OU=HR_Department,DC=lab04,DC=lan"
Added ou "OU=HR_Department,DC=lab04,DC=lan"
sergio@ls04:~$ sudo samba-tool ou create "OU=Students,DC=lab04,DC=lan"
Added ou "OU=Students,DC=lab04,DC=lan"
```

Mover Usuarios y Grupos a sus OUs:

Usuario:

```
sudo samba-tool user move alice "OU=IT_departaments,DC=lab04,DC=lan"
```

```
sudo samba-tool user move bob "OU=Students,DC=lab04,DC=lan"
```

```
sudo samba-tool user move charlie "OU=HR_Department,DC=lab04,DC=lan"
```

Grupos:

```
sudo samba-tool group move IT_admins "OU=IT_departaments,DC=lab04,DC=lan"
```

```
sudo samba-tool group move Students "OU=Students,DC=lab04,DC=lan"
```

```
sudo samba-tool group move IT_departaments "OU=HR_Department,DC=lab04,DC=lan"
```

```
sergio@ls04:~$ sudo samba-tool user move alice "OU=IT_departaments,DC=lab04,DC=lan"
Moved user "alice" into "OU=IT_departaments,DC=lab04,DC=lan"
sergio@ls04:~$ sudo samba-tool user move bob "OU=Students,DC=lab04,DC=lan"
Moved user "bob" into "OU=Students,DC=lab04,DC=lan"
sergio@ls04:~$ sudo samba-tool group move IT_admins "OU=IT_departaments,DC=lab04,DC=lan"
Moved group "IT_admins" into "OU=IT_departaments,DC=lab04,DC=lan"
sergio@ls04:~$ sudo samba-tool group move Students "OU=Students,DC=lab04,DC=lan"
Moved group "Students" into "OU=Students,DC=lab04,DC=lan"
sergio@ls04:~$
```

Verificar :

sudo samba-tool ou list

```
sergio@ls04:~$ sudo samba-tool ou list
OU=Students
OU=HR_Department
OU=IT_departaments
OU=Domain Controllers
sergio@ls04:~$ sudo samba-tool user show alice | grep dn
dn: CN=alice,OU=IT_departaments,DC=lab04,DC=lan
```

Crear la GPO en el Servidor Samba :

Samba permite crear el objeto GPO aunque sea para clientes Linux. En el servidor:

Crear la GPO :

```
sudo samba-tool gpo create "IT_Security_Policy" -U Administrator
```

```
sergio@ls04:~$ sudo samba-tool gpo create "IT_Security_Policy" -U Administrator
[sudo] password for sergio:
WARNING: Using passwords on command line is insecure. Installing the setproctitle python module will hide these from shortly after program start.
Password for [LAB04\Administrator]:
Using temporary directory /tmp/tmpnj8f90x8 (use --tmpdir to change)
GPO 'IT Security Policy' created as {6DCC05BC-2848-4F4E-89E4-44EBE1A4C823}
```

Crear la PSO para la OU de IT_departaments

```
sudo samba-tool domain passwordsettings pso create "PSO_IT_Estricta" 10
--account-lockout-threshold=3 --account-lockout-duration=5
--reset-account-lockout-after=5 -U Administrator
```

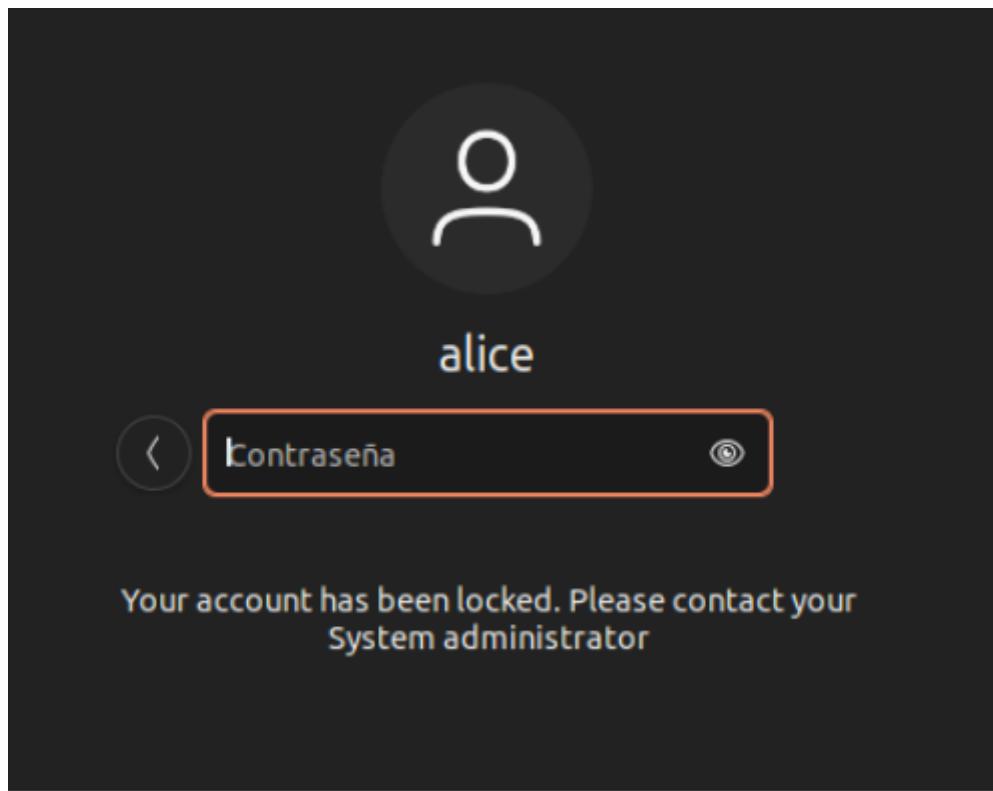
Este comando define las reglas de 3 intentos y 5 minutos de bloqueo.

```
sergio@ls04:~$ sudo samba-tool domain passwordsettings pso create "PSO_IT_Estricta" 10 --account-lockout-threshold=3 --account-lockout-duration=5 --reset-account-lockout-after=5 -U Administrator
[sudo] password for sergio:
WARNING: Using passwords on command line is insecure. Installing the setproctitle python module will hide these from shortly after program start.
Not all password policy options have been specified.
For unspecified options, the current domain password settings will be used as the default values.
PSO successfully created: CN=PSO_IT_Estricta,CN=Password Settings Container,CN=System,DC=lab04,DC=lan
Password information for PSO 'PSO_IT_Estricta'

Precedence (lowest is best): 10
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 8
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 5
Account lockout threshold (attempts): 3
Reset account lockout after (mins): 5
```

Aplicar la SPO al grupo ya que samba esta diseñado para aplicar al grupo que contiene los usuarios

```
sudo samba-tool domain passwordsettings pso apply "PSO_IT_Estricta" "it_admins"
-U Administrator
```



SPRINT 3 Creación y compartición de carpeta

1. En el Servidor: Crear carpetas (Finance, HRdosc, Public) y configurar Samba

sudo mkdir -p /srv/samba/Finance

```
sergio@ls04:~$ sudo mkdir -p /srv/samba/Finance
[sudo] password for sergio:
sergio@ls04:~$ sudo mkdir -p /srv/samba/HRdosc
sergio@ls04:~$ sudo mkdir -p /srv/samba/Public
sergio@ls04:~$
```

Configurar el recurso en

sudo nano /etc/samba/smb.conf

Añadir al final del archivo:

Dns del instituto 10.239.3.7

```
# Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = LS04
    realm = LAB04.LAN
    server role = active directory domain controller
    workgroup = LAB04

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

[netlogon]
    path = /var/lib/samba/sysvol/lab04.lan/scripts
    read only = No
[Finance]
    path = /srv/samba/Finance
    read only = No

[HRdocs]
    path = /srv/samba/HRdocs
    read only = No

[Public]
    path = /srv/samba/Public
    read only = No
```

```
[Finance]
path = /srv/samba/Finance
read only = No
```

Añade las carpetas:

Reiniciar samba:

```
sudo systemctl restart smbd
```

2. En el Servidor: Aplicar Permisos de Disco (ACLs)

Primero instalar las herramientas de ACLs

```
sudo apt update && sudo apt install acl -y
```

```
sudo setfacl -m g:"LAB04\IT_admins":rwx /srv/samba/Finance
```

Al ejecutar el comando para dar los permisos a las carpetas tendrá problemas de argumentos invalidos, ver algunons comprobaciones:

```
getent group | grep -i IT_admins
```

Este comando verificará la el grupo en ubuntu AD, si no sale nada es porque no está resolviendo los usuarios de AD

Modificar **sudo nano /etc/samba/smb.conf** añadir las siguientes líneas específicas para controladores de dominio:

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

```

# Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = LS04
    realm = LAB04.LAN
    server role = active directory domain controller
    workgroup = LAB04

#Añadir estas lineas para el mapeo

winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes

idmap_idb:use xid = yes
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes

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

[netlogon]
    path = /var/lib/samba/sysvol/lab04.lan/scripts
    read only = No

[Finance]
    path = /srv/samba/Finance
    read only = No

[HRdocs]
    path = /srv/samba/HRdocs
    read only = No

[Public]
    path = /srv/samba/Public
    read only = No

```

#Añadir estas líneas para el mapeo

```

winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes

```

```
idmap_ldb:use xid = yes  
winbind enum users = yes  
winbind enum groups = yes  
winbind use default domain = yes
```

Forzar la vinculación de librerías NSS

Ubuntu no registra la ubicación de la librería, usar estos comandos para refrescar el sistema:

```
sudo ln -sf /lib/x86_64-linux-gnu/libnss_winbind.so.2  
/lib/x86_64-linux-gnu/libnss_winbind.so
```

sudo ldconfig

```
sergio@ls04:~$ sudo ln -sf /lib/x86_64-linux-gnu/libnss_winbind.so.2 /lib/x86_64-linux-gnu/libnss_winbi  
nd.so  
sergio@ls04:~$ sudo ldconfig  
sergio@ls04:~$ █
```

Limpieza de Caché y Reinicio Total

Detener el servicio

sudo systemctl stop samba-ad-dc

Limpiar cachés de identidades

sudo net cache flush

sudo rm -f /var/lib/samba/*.tdb

sudo rm -f /var/lib/samba/group_mapping.tdb

Iniciar el servicio

sudo systemctl start samba-ad-dc

```
sergio@ls04:~$ sudo net cache flush
sergio@ls04:~$ sudo rm -f /var/lib/samba/*.tdb
sergio@ls04:~$ sudo rm -f /var/lib/samba/group_mapping.tdb
sergio@ls04:~$ sudo systemctl start samba-ad-dc
[sergio@ls04:~$ ]
```

Ahora este comando NO fallará

```
sudo setfacl -m g:it_admins:rwx /srv/samba/Finance
```

Si te falla Intenta esto:

```
getent group it_admins
```

```
getent group "LAB04\it_admins"
```

Si te salen los grupos prueba esto :

```
sudo nano /etc/nsswitch.conf
```

```
GNU nano 7.2                               /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:      files  systemd  winbind
group:       files  systemd  winbind
shadow:      files  systemd
gshadow:     files  systemd

hosts:        files  dns
networks:    files

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

netgroup:    nis
```

Para que Linux entienda lo que dice **winbind**, necesita una librería específica. Si no la tienes, **getent** seguirá fallando. Instálala con:

```
sudo apt update
```

```
sudo apt install libnss-winbind libpam-winbind
```

Ahora reinicia los servicios para que lean la nueva configuración:

```
sudo systemctl restart winbind
```

```
sudo systemctl restart smbd nmbd
```

Ahora ejecuta de nuevo:

```
getent group "LAB04\it_admins"
```

```
sergio@ls04:~$ getent group "LAB04\it_admins"
LAB04\it_admins:x:3000021:
sergio@ls04:~$ █
```

Ejecutar el **setfacl** correctamente

Una vez que **getent** funcione, lanza el comando de esta forma (usando comillas simples para que la barra \ no dé problemas):

Bash

```
sudo setfacl -m 'g:LAB04\it_admins:rwx' /srv/samba/Finance
```

```
sudo setfacl -m g:it_admins:rwx /srv/samba/HRdocs
```

```
sudo setfacl -m g:it_admins:rwx /srv/samba/Public
```

```
LAB04\Students
sergio@ls04:~$ sudo setfacl -m g:it_admins:rwx /srv/samba/HRdocs
sergio@ls04:~$ sudo setfacl -m g:it_admins:rwx /srv/samba/Public
sergio@ls04:~$ █
```

Permisos para **Students** (Bob - Acceso restringido)

Bob y su grupo solo pueden modificar **Public**. En las demás, solo pueden ver el contenido (lectura y ejecución para entrar en la carpeta).

Bash

```
# En Public: Permiso de Lectura y Escritura
```

```
sudo setfacl -m g:students:rwx /srv/samba/Public
```

```
# En Finance y HRdocs: Solo Lectura (rx)
```

```
sudo setfacl -m g:students:rx /srv/samba/Finance
```

```
sudo setfacl -m g:students:rx /srv/samba/HRdocs
```

```
sergio@ls04:~$ sudo setfacl -m g:students:rwx /srv/samba/Public  
sergio@ls04:~$ sudo setfacl -m g:students:rx /srv/samba/Finance
```

3. Permisos para IT_departaments (Charlie - Acceso Selectivo)

Charlie puede modificar su carpeta de RRHH y la pública, pero no tiene acceso a Finanzas.

Bash

```
# En HRdocs: Permiso de Lectura y Escritura
```

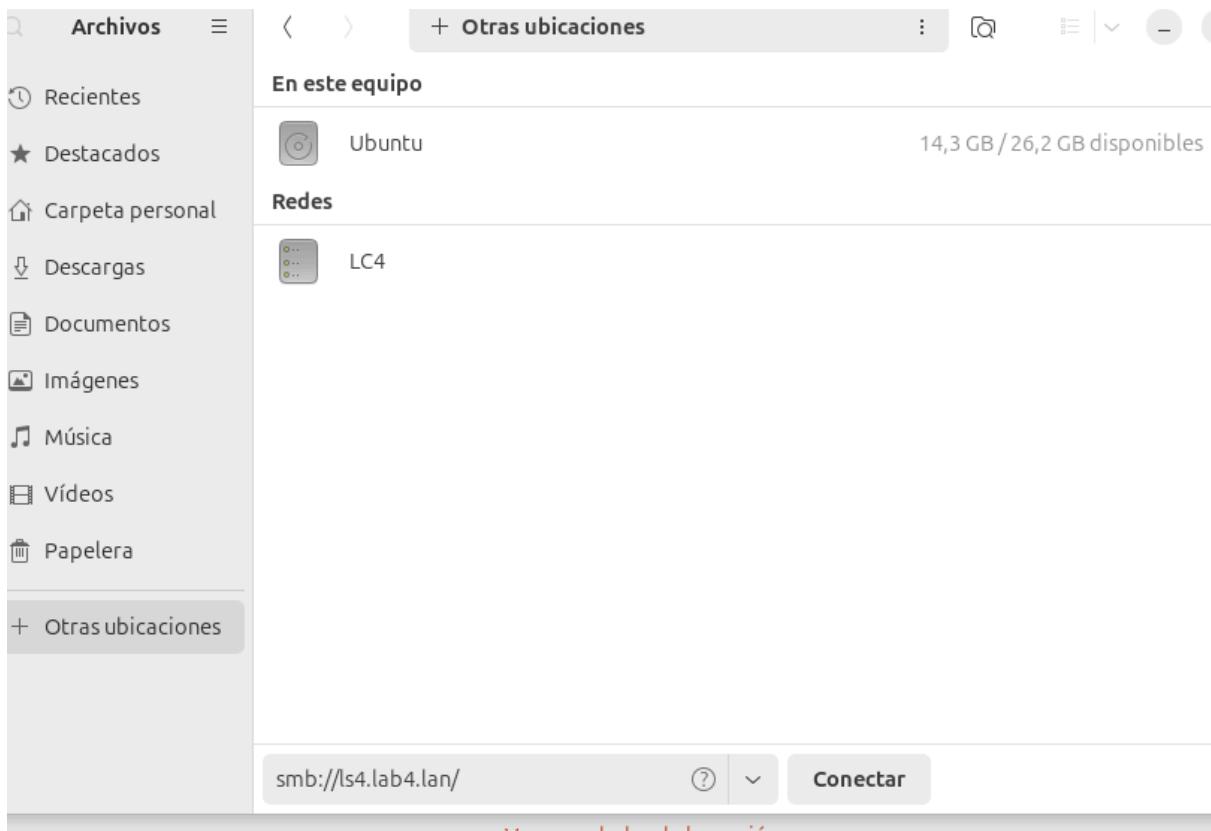
```
sudo setfacl -m g:it_departaments:rwx /srv/samba/HRdocs
```

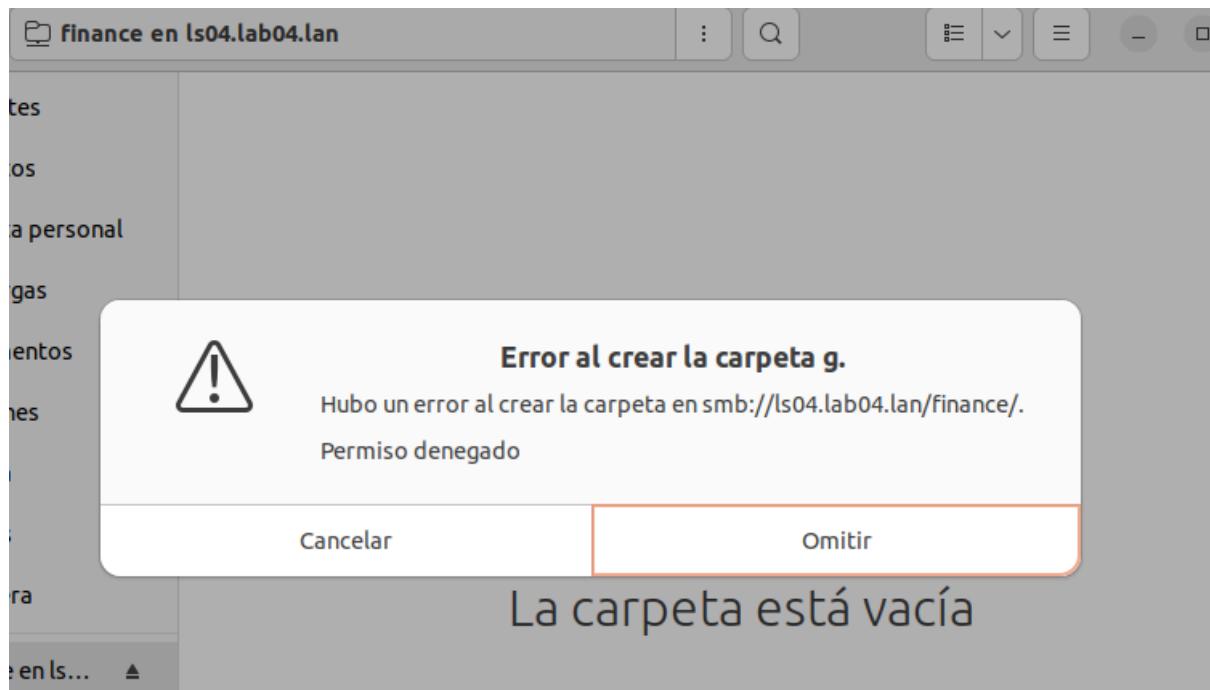
```
# En Public: Permiso de Lectura y Escritura
```

```
sudo setfacl -m g:it_departaments:rwx /srv/samba/Public
```

```
# En Finance: Denegar acceso total (quitar todos los permisos)
```

```
sudo setfacl -m g:it_departaments:--- /srv/samba/Finance
```





Preparación del Disco (Equivalente a Administración de Discos)

Agregar un disco de 10Gb e identificar en la servidor

```
sergio@ls04:~$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda        8:0    0   40G  0 disk 
└─sda1     8:1    0    1M  0 part 
  ├─sda2     8:2    0    2G  0 part /boot
  ├─sda3     8:3    0   38G  0 part 
    └─ubuntu--vg-ubuntu--lv 252:0    0   19G  0 lvm   /
sdb        8:16   0   10G  0 disk 
sr0       11:0    1 1024M 0 rom 
sergio@ls04:~$
```

Crear tabla de particiones GPT y una partición primaria

```
sudo parted /dev/sdb mklabel gpt
```

```
sudo parted /dev/sdb mkpart primary ext4 0% 100%
```

```
sergio@ls04:~$ sudo parted /dev/sdb mklabel gpt
[sudo] password for sergio:
Information: You may need to update /etc/fstab.

sergio@ls04:~$ sudo parted /dev/sdb mkpart primary ext4 0% 100%
Information: You may need to update /etc/fstab.

sergio@ls04:~$
```

Formatear y Asignar Etiqueta (Equivalente a NTFS y DataDrive): En Linux usamos **EXT4** por ser el estándar nativo, aunque Samba lo presentará a los clientes como NTFS.

Formatear el disco sdb1

sudo mkfs.ext4 -L Datadrive /dev/sdb1

```
sergio@ls04:~$ sudo mkfs.ext4 -L Datadrive /dev/sdb1
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 612058ea-f7d7-420b-ac59-c91b936e8462
Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

sergio@ls04:~$
```

Montar el disco y Mover Carpetas (Equivalente a D:\Shares): En Linux no usamos **D:**, sino que "montamos" el disco en una carpeta del sistema.

sudo mkdir -p /mnt/Datadrive

sudo mount /dev/sdb1 /mnt/Datadrive

```
sergio@ls04:~$ sudo mkdir -p /mnt/Datadrive
sergio@ls04:~$ sudo mount /dev/sdb1 /mnt/Datadrive
sergio@ls04:~$
```

Crear la estructura de carpetas

sudo mkdir -p /mnt/Datadrive/shares/Finance

sudo mkdir -p /mnt/Datadrive/shares/HRdocs

```
sudo mkdir -p /mnt/Datadrive/shares/Public
```

Mover los contenidos de /srv/samba > /mnt/Datadrive/shares/

```
sudo mv /srv/samba/* /mnt/Datadrive/shares/
```

Configurar el archivo **sudo nano /etc/fstab** > agregar al final de todo

```
sudo nano /etc/fstab
```

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/ubuntu-vg/ubuntu-lv during curtin installation
/dev/disk/by-id/dm-uuid-LVM-kS10VxIC5z5xkJh5w3kEw34kHZTlfc2syn0IgEcrJ2nfccdrLb4o12XNo1ws6ZAd / ext4 defaults 0 1
# /boot was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/c2468a9d-6e4b-4a39-b049-082e106d100f /boot ext4 defaults 0 1
/swap.img none swap sw 0 0
LABEL=DataDrive /mnt/DataDrive ex4 defaults 0 2
```

LABEL=Datadrive /mnt/Datadrive ex4 defaults 0 2

Actualizar **sudo nano /etc/samba/smb.conf** ya que las carpetas están en un nuevo disco

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

```
[Finance]
    path = /mnt/Datadrive/shares/Finance
    read only = No

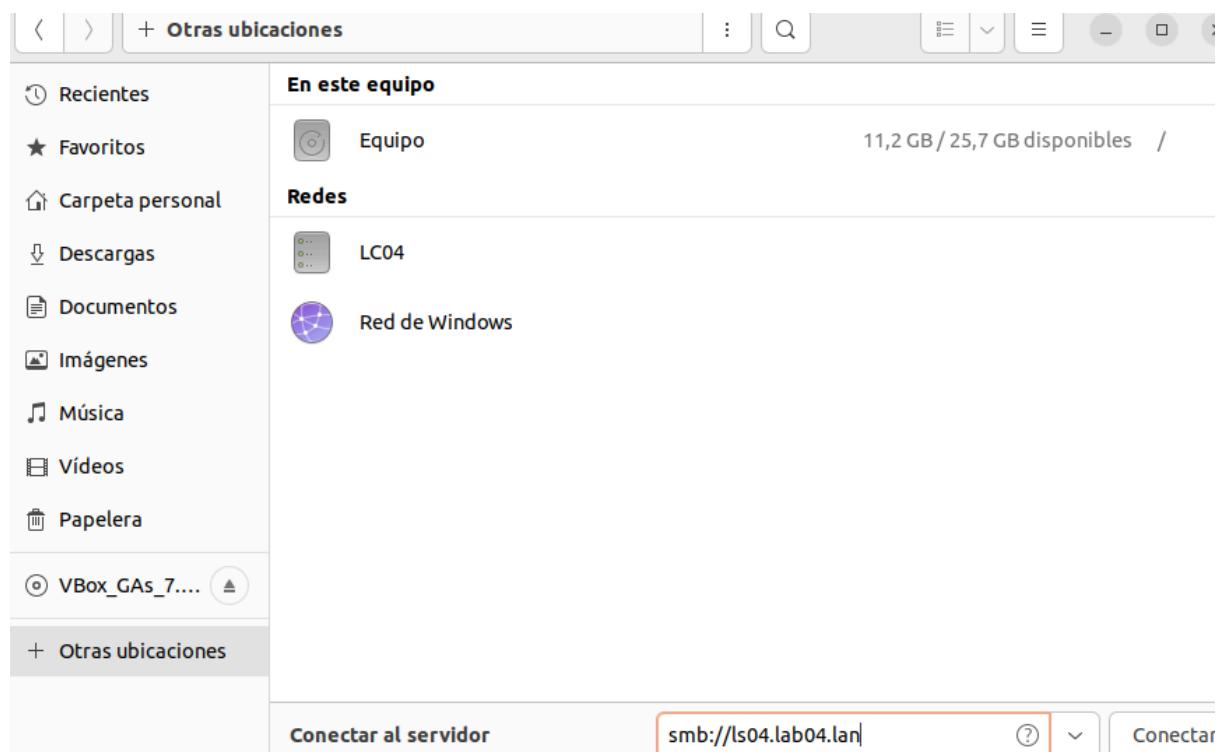
[HRdocs]
    path = /mnt/Datadrive/shares/HRdocs
    read only = No

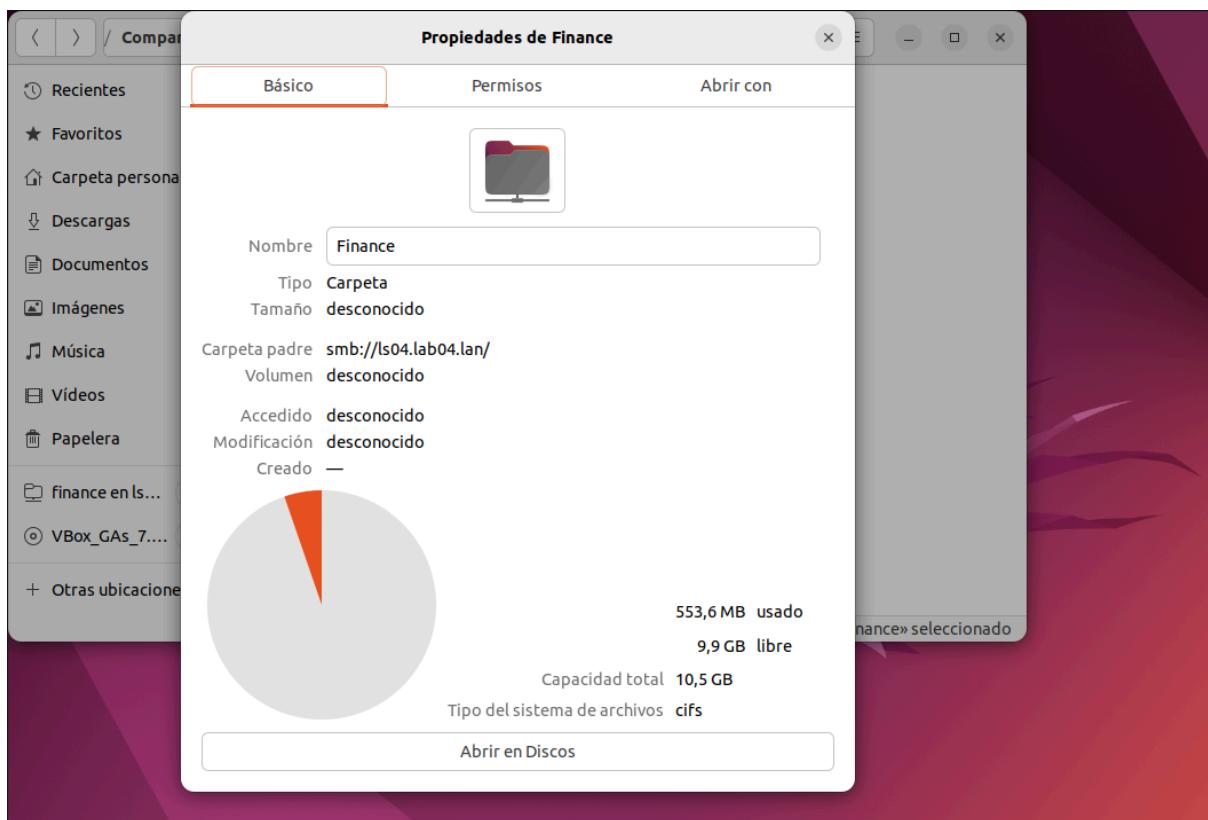
[Public]
    path = /mnt/Datadrive/shares/Public
    read only = No
```

Reiniciar samba >

sudo systemctl restart samba-ad-dc

Comprobar con cualquiera de los usuarios





Crear Tarea Programada (Backup)

sudo nano /root/backup.sh y agregar el siguiente contenido

sudo nano /root/backup.sh

```
#!/bin/bash
fecha=$(date +%Y-%m-%d)
echo "Iniciando backup de Finance el $fecha..." >> /var/log/backup_laboratorio.log
tar -czf /mnt/Datadrive/backup_finance_$fecha.tar.gz /mnt/Datadrive/shares/Finance
echo "Backup completado exitosamente." >> /var/log/backup_laboratorio.log
```

```
GNU nano 2.2                               /root/backup.sh
#!/bin/bash
fecha=$(date +%Y-%m-%d)
echo "Iniciando backup de Finance el $fecha..." >> /var/log/backup_laboratorio.log
tar -czf /mnt/Datadrive/backup_finance_$fecha.tar.gz /mnt/Datadrive/shares/Finance
echo "Backup completado exitosamente." >> /var/log/backup_laboratorio.log
```

Dar los permisos de ejecución al script
Programar la tarea 7pm diariamente >

sudo crontab -e

> primero le das enter y añadir al final de todo

```
0 19 * * * /root/backup.sh
```

```
# m h dom mon dow command
0 19 * * * /root/backup.sh
```

Seguridad y Auditoría básica

Para generar un evento de auditoría en los logs de Samba:

Habilitar en el servidor: Revisa que en `smb.conf` la carpeta `[Finance]` tenga:

`vfs objects = full_audit`

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

[netlogon]
    path = /var/lib/samba/sysvol/lab04.lan/script
    read only = No

[Finance]
    path = /mnt/Datadrive/shares/Finance
    read only = No
    vfs objects = full_audit

[HRdocs]
    path = /mnt/Datadrive/shares/HRdocs
    read only = No

[Public]
    path = /mnt/Datadrive/shares/Public
    read only = No
```

Tienes que poner otra vez los permisos por si a caso. Pero con la nueva ruta

```
sudo setfacl -m 'g:LAB04\it_admins:rwx' /mnt/Datadrive/shares/Finance
```

Luego intentar entrar con Alice a la carpeta Finance e intentar crear borrar y luego en el servidor comprobar el visor de tareas si no sale nada con el comando para ver el visor de tareas hay que configurar smb.conf otra vez.

Lo del tren:

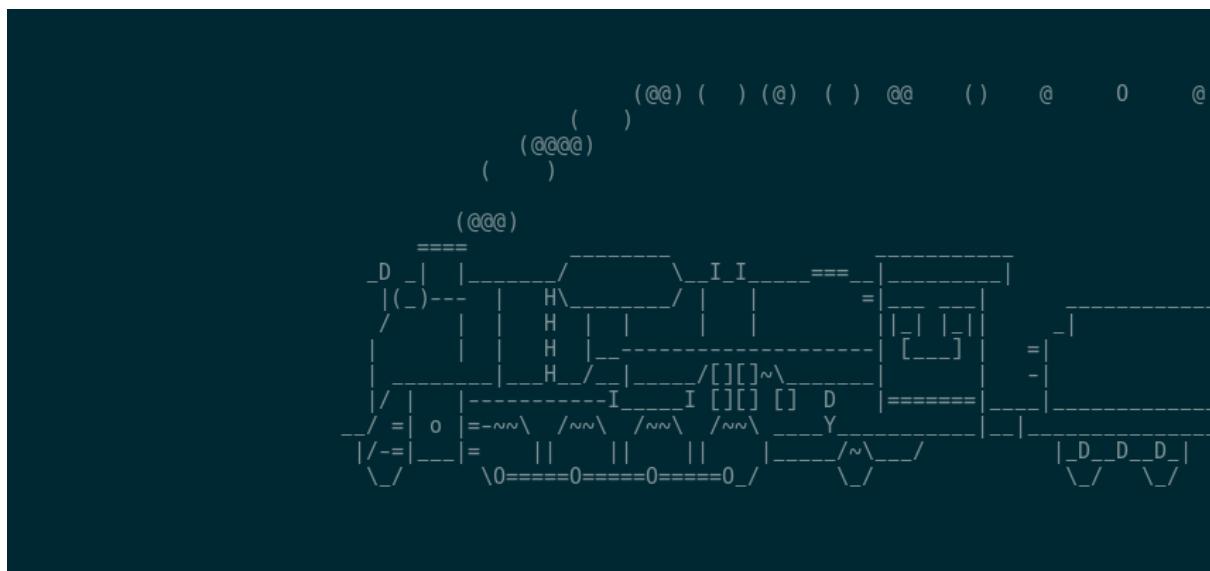
Instala:

```
sudo apt update
```

```
sudo apt install sl
```

Para iniciar el tren es con:En el server

sl



RECUERDA :Poner el ssh en el cliente.

Instalar:

```
sudo apt update
```

```
sudo apt install openssh-server
```

Para entrar:

ssh sergio@172.30.20.39

En el Cliente: Habres dos terminales

En una pones:

ps aux

Y en la otra para parar:

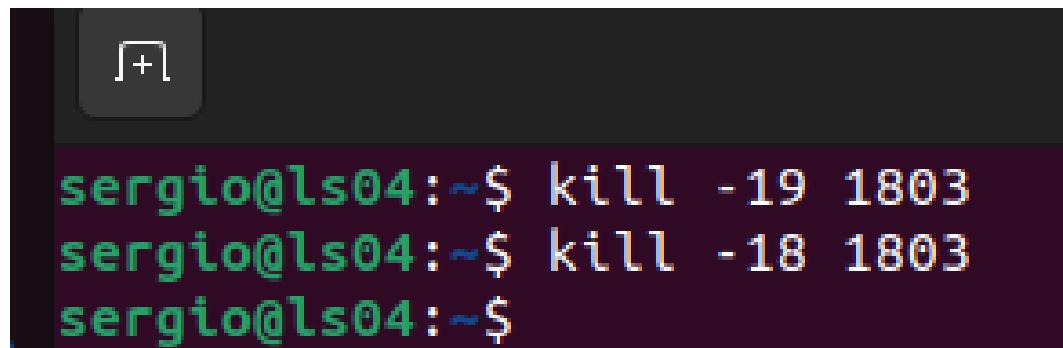
kill -19 y el número de ps aux

```
[+] sergio@ls04:~$ kill -19 1803
sergio@ls04:~$ █

root      1/11  0.0  0.0      0      0 ?          1    08:32  0:00 [KWORKER
root     1733  0.0  0.2  15324 10624 ?          Ss   08:36  0:00 sshd: s
sergio    1789  0.0  0.1  15324  7692 ?          S    08:36  0:00 sshd: s
sergio    1790  0.0  0.1   8648  5376 pts/2      Ss+  08:36  0:00 -bash
sergio    1803  0.0  0.0   3068  2176 pts/0      S+   08:37  0:00 sl
sergio    1804  0.0  0.1  10884  4480 pts/1      R+   08:37  0:00 ps aux
sergio@ls04:~$ █
```

Y para reanudar es :

kill -18 y el número de ps aux



```
sergio@ls04:~$ kill -19 1803
sergio@ls04:~$ kill -18 1803
sergio@ls04:~$
```

Creación de la Relación de Confianza (Trust)

Primero:

sudo nano /etc/samba/smb.conf

```
[global]
# Global parameters
dns forwarder = 10.239.3.7 192.168.10.16
netbios name = LS4
realm = LAB4.LAN
server role = active directory domain controller
workgroup = LAB4

winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes

idmap_ldb:use xid = yes
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes

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

[netlogon]
path = /var/lib/samba/sysvol/lab4.lan/scripts
read only = No

[Hola1]
path = /mnt/Datadrive/shares/Hola1
read only = No
```

Segundo:

sudo nano /etc/hosts

```
GNU nano 7.2                                     /etc/hosts
127.0.0.1 localhost
127.0.1.1 admin
192.168.10.117 ls4.lab4.lan ls4
192.168.10.120 ls2044.lab2044.lan ls2044
# 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
```

sudo nano /etc/resolv.conf

sudo chattr -i /etc/resolv.conf

```
GNU nano 7.2                                     /etc/resolv.conf
nameserver 192.168.10.120
nameserver 192.168.10.117
nameserver 10.239.3.7
search lab4.lan
```

sudo chattr +i /etc/resolv.conf

Restart Service

sudo systemctl restart samba-ad-dc

sudo timedatectl set-ntp true

Usaremos el comando samba-tool para crear una confianza de bosque bidireccional.
Este comando se ejecuta en LS04.

```
sudo samba-tool domain trust create lab2044.lan \
--type=forest \
--direction=both \
--create-location=both \
--user=Administrator@lab2044.lan
```

Ingresar la contraseña del otro dominio:

```

sergio@ls04:~$ sudo samba-tool domain trust create lab2044.lan \
--type=forest \
--direction=both \
--create-location=both \
--user=Administrator@lab2044.lan
WARNING: Using passwords on command line is insecure. Installing the setproctitle python module will hide these from shortly after program start.
LocalDomain Netbios[LAB04] DNS[lab04.lan] SID[S-1-5-21-2394689947-2037422089-3061927611]
RemoteDC Netbios[LS2044] DNS[ls2044.lab2044.lan] ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET_DOMAIN_6]
Password for [Administrator@lab2044.lan]:
RemoteDomain Netbios[LAB2044] DNS[lab2044.lan] SID[S-1-5-21-1518338840-2647584163-27716547]
Creating remote TDO.
Remote TDO created.
Setting supported encryption types on remote TDO.
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
Namespaces[2] TDO[lab2044.lan]:
TLN: Status[Enabled]           DNS[*.lab2044.lan]
DOM: Status[Enabled]           DNS[lab2044.lan] Netbios[LAB2044] SID[S-1-5-21-1518338840-2647584163-27716547]
Setup remote forest trust information...
Namespaces[2] TDO[lab04.lan]:
TLN: Status[Enabled]           DNS[*.lab04.lan]
DOM: Status[Enabled]           DNS[lab04.lan] Netbios[LAB04] SID[S-1-5-21-2394689947-2037422089-3061927611]
Validating outgoing trust...
OK: LocalValidation: DC[\ls2044.lab2044.lan] CONNECTION[WERR_OK] TRUST[WERR_OK] VERIFY_STATUS_RETURNED
Validating incoming trust...
OK: RemoteValidation: DC[\ls04.lab04.lan] CONNECTION[WERR_OK] TRUST[WERR_OK] VERIFY_STATUS_RETURNED
Success.
sergio@ls04:~$ 
```

Pruebas de Validación

Una vez creada la confianza, debemos comprobar que los dominios "confían" el uno en el otro.

En ls04 comprobar:

sudo samba-tool domain trust list

```

sergio@ls04:~$ sudo samba-tool domain trust list
Type[Forest]  Transitive[Yes] Direction[BOTH]      Name[lab2044.lan]
sergio@ls04:~$ 
```

y en ls2044:

```

sergio@ls2044:~$ sudo samba-tool domain trust list
Type[Forest]  Transitive[Yes] Direction[BOTH]      Name[lab04.lan]
sergio@ls2044:~$ 
```

Prueba de resolución cruzada (nslookup) en ambos servidores:

nslookup

```
sergio@ls04:~$ nslookup lab2044.lan
Server:      192.168.10.120
Address:     192.168.10.120#53

Name:   lab2044.lan
Address: 172.30.20.120
Name:   lab2044.lan
Address: 192.168.10.120

sergio@ls04:~$ █
```

```
sergio@ls2044:~$ nslookup lab04.lan
Server:      192.168.10.37
Address:     192.168.10.37#53

Name:   lab04.lan
Address: 172.30.20.39
Name:   lab04.lan
Address: 192.168.10.37

sergio@ls2044:~$ █
```

Verificar resolución de usuarios remotos (Winbind):

sudo samba-tool user list -H ldap://lab2044.lan -U Administrator

```
sergio@ls04:~$ sudo samba-tool user list -H ldap://lab2044.lan -U Administrator
WARNING: Using passwords on command line is insecure. Installing the setproctitle python module will hide this
from shortly after program start.
Password for [LAB04\Administrator]:
Guest
krbtgt
Administrator
sergio@ls04:~$ █
```

sudo samba-tool user list -H ldap://lab04.lan -U Administrator

```
sergio@ls2044:~$ sudo samba-tool user list -H ldap://lab04.lan -U Administrator
Password for [LAB2044\Administrator]:
alice
Administrator
bob
Guest
charlie
krbtgt
sergio@ls2044:~$ █
```

Para unir un cliente al otro Dominio.

Por si acaso haz esto en el server principal:

```
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

En el Cliente:

Primero:

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

```
GNU nano 6.2                               /etc/hosts *
127.0.0.1      localhost
127.0.1.1      lc04
192.168.10.37   lab04.lan
192.168.10.37   ls04.lab04.lan  ls04
192.168.10.120  ls2044.lab2044.lan ls2044
# 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
```

Haz un backup:

```
sudo mv /etc/resolv.conf /etc/resolv.conf.backup
```

```
sergio@lc04:~$ sudo mv /etc/resolv.conf /etc/resolv.conf.backup
```

Después pones esto:

```
sudo nano /etc/resolv.conf
```

```
GNU nano 6.2                               /etc/resolv.conf *
nameserver 192.168.10.120
nameserver 192.168.10.37
```

nameserver 192.168.10

nameserver 192.168.10

Cierra sesión y haz esto: En el segundo server crea clientes.

```
sudo samba-tool user create paco
```

```
sergio@ls2044:~$ sudo samba-tool user create paco
[sudo] password for sergio:
New Password:
Retype Password:
User 'paco' added successfully
sergio@ls2044:~$ sudo samba-tool user create hola
New Password:
Retype Password:
User 'hola' added successfully
sergio@ls2044:~$ sudo samba-tool user create vegetta
New Password:
Retype Password:
User 'vegetta' added successfully
sergio@ls2044:~$ █
```

Para comprobar los clientes que tienes en el server dos:

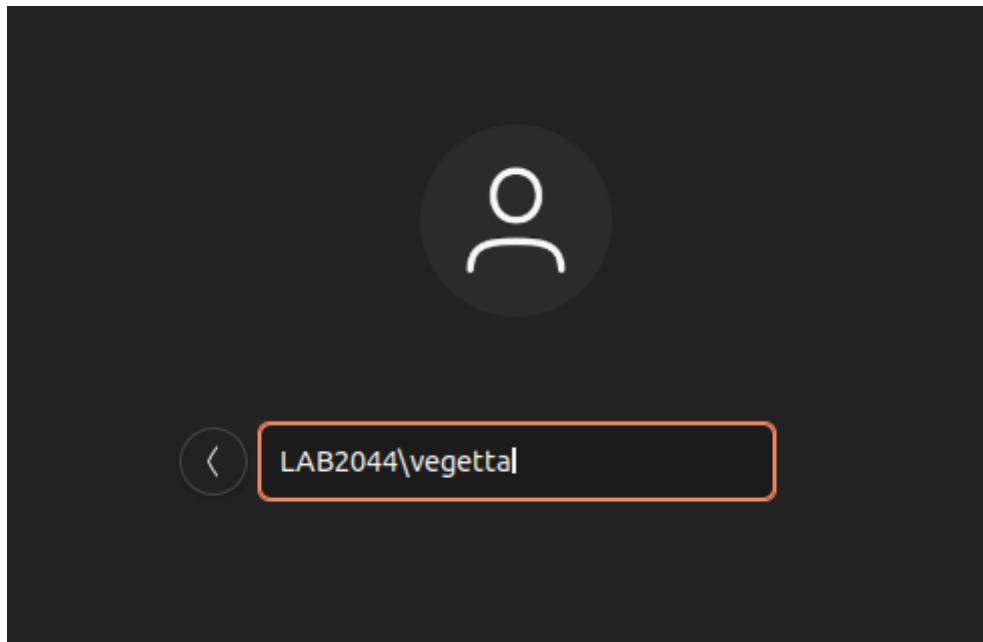
```
wbinfo -u
```

```
sergio@ls2044:~$ wbinfo -u
LAB2044\administrator
LAB2044\guest
LAB2044\krbtgt
LAB2044\paco
LAB2044\hola
LAB2044\vegetta
sergio@ls2044:~$ █
```

En el server primero:

```
sergio@ls04:~$ wbinfo -u
LAB04\administrator
LAB04\guest
LAB04\krbtgt
LAB04\alice
LAB04\bob
LAB04\charlie
sergio@ls04:~$ █
```

Y ahora en el cliente cierras sesión : Inicias con un cliente del server dos.



```
LAB2044\vegetta@lc04:~$
```

Preparar servidor para Samba AD AWS

Configurar el hostname y la IP fija
sudo hostnamectl set-hostname ls204
luego dentro de
sudo nano /etc/hosts

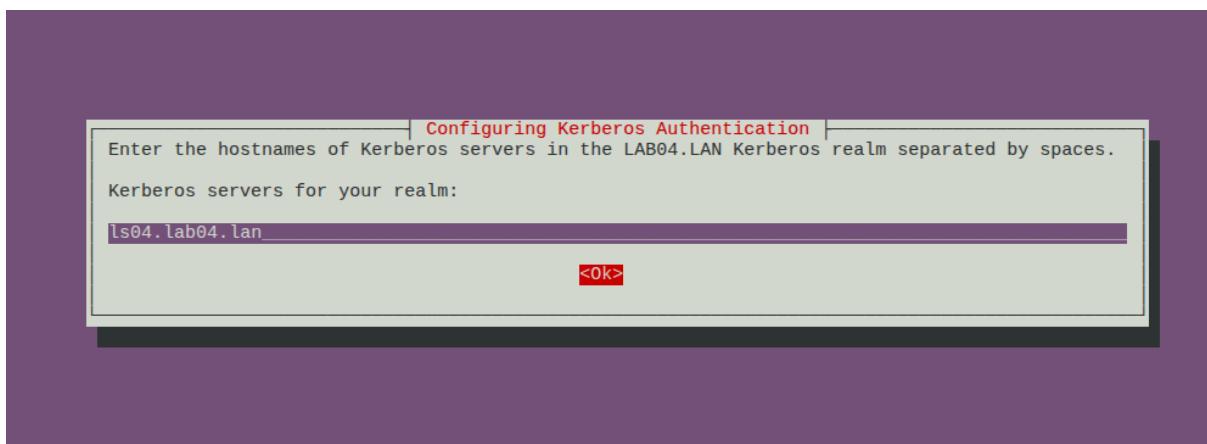
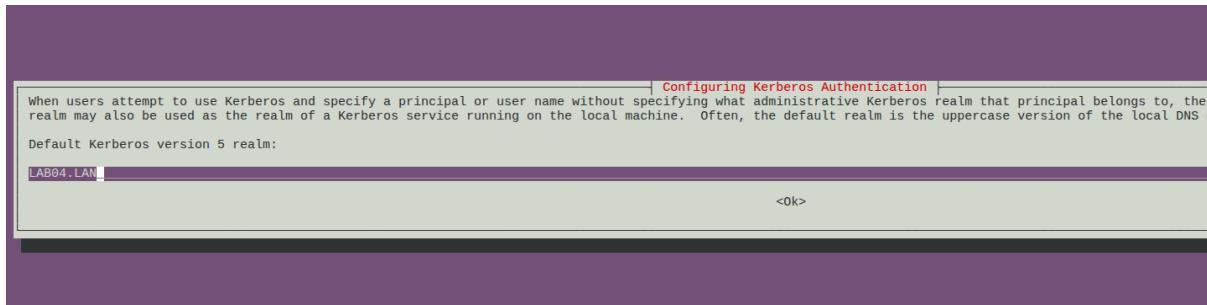
su reboot

Con los siguientes comandos instalar samba:

sudo apt update

**sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules
smbclient winbind libpam-winbind libnss-winbind libpam-krb5 krb5-config
krb5-user dnsutils chrony net-tools**

Durante la instalación pedirá el dominio de servidores para kerberos, poner el dominio:



Deshabilitar servicios Samba clásicos

Detener y deshabilitar los servicios que Active Directory que no se van a usar.

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

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

```
ubuntu@ip-172-31-31-175:~$ sudo systemctl stop smbd nmbd winbind
ubuntu@ip-172-31-31-175:~$ sudo systemctl disable smbd nmbd winbind
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/multi-user.target.wants/smbd.service".
Removed "/etc/systemd/system/multi-user.target.wants/nmbd.service".
Removed "/etc/systemd/system/multi-user.target.wants/winbind.service".
Removed "/etc/systemd/system/smb.service".
Removed "/etc/systemd/system/nmb.service".
ubuntu@ip-172-31-31-175:~$
```

El servidor solo necesita samba ad-dc para funcionar como Active Directory

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

Crear una copia de seguridad del archivo **/etc/samba/sab.conf**
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak

FASE 5 — Provisionar el AD Samba

Ejecutar provisionado

Ejecutar el comando **sudo samba-tool domain provision**

Luego Crear copia de seguridad de la configuración predeterminada de kerberos
sudo mv /etc/krb5.conf /etc/krb5.conf.orig

Reemplazar con el archivo /var/lib/samba/krb5.conf
sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf

No edite nada lo deje porque ya estaba configurado

```
sudo nano /etc/krb5.conf
```

FASE 6 - Activar el controlador de dominio

Iniciar servicio samba Active Directory samba-ad-dc

sudo systemctl start samba-ad-dc

Comprobar servicios

sudo systemctl status samba-ad-dc

```
● samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/usr/lib/systemd/system/samba-ad-dc.service; enabled; preset: enabled)
   Active: active (running) since Fri 2026-02-13 08:50:11 UTC; 13s ago
     Docs: man:samba(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 6556 ExecCondition=/usr/share/samba/is-configured samba (code=exited, status=0/SUCCESS)
 Main PID: 6559 (samba)
   Status: "samba: ready to serve connections..."
    Tasks: 58 (limit: 1008)
   Memory: 184.7M (peak: 261.8M)
      CPU: 3.821s
 CGroup: /system.slice/samba-ad-dc.service
         ├─6559 "samba: root process"
         ├─6560 "samba: tfork waiter process(6561)"
         ├─6561 "samba: task[s3fs] pre-fork master"
         ├─6562 "samba: tfork waiter process(6564)"
         ├─6563 "samba: tfork waiter process(6566)"
         ├─6564 "samba: task[rpc] pre-fork master"
         ├─6565 "samba: tfork waiter process(6568)"
         ├─6566 /usr/sbin/smbd -D "--option=server role check:inhibit=yes" --foreground
         ├─6567 "samba: tfork waiter process(6569)"
         ├─6568 "samba: task[nbt] pre-fork master"
         ├─6569 "samba: task[rpc] pre-forked worker(0)"
         ├─6570 "samba: tfork waiter process(6572)"
         ├─6571 "samba: tfork waiter process(6573)"
         ├─6572 "samba: task[wrepl] pre-fork master"
         ├─6573 "samba: task[rpc] pre-forked worker(1)"
         ├─6574 "samba: tfork waiter process(6577)"
         ├─6575 "samba: tfork waiter process(6576)"
         ├─6576 "samba: task[rpc] pre-forked worker(2)"
         ├─6577 "samba: task[ldap] pre-fork master"
         ├─6578 "samba: tfork waiter process(6579)"
         ├─6579 "samba: task[rpc] pre-forked worker(3)"
         ├─6580 "samba: tfork waiter process(6581)"
         ├─6581 "samba: task[cldap] pre-fork master"
         ├─6582 "samba: tfork waiter process(6584)"
         ├─6584 "samba: task[kdc] pre-fork master"
         ├─6585 "samba: tfork waiter process(6587)"
         ├─6586 "samba: tfork waiter process(6588)"

Lines 1-40 [ctrl-C]
```

Antes debo deshabilitar el archivo resolv

sudo systemctl disable --now systemd-resolved es donde apunta a mi servidor para resolver los nombres de dominios ya que voy a implementar el servidor samba por que es incompatible.

Lo siguiente es eliminar el enlace simbólico **sudo unlink /etc/resolv.conf** las modificaciones que se hagan en este ya no se hagan si no en el verdadero.

Crear un nuevo fichero resolv.conf

sudo nano /etc/resolv.conf

```
GNU nano 7.2
nameserver 172.31.31.175
nameserver 8.8.8.8
search lab04.lan
```

ahora hacemos inmutable el archivo /etc/resolv.conf para que no pueda cambiar
sudo chattr +i /etc/resolv.conf

FASE 7 — Validación Final

Comprobar autenticación en el servidor de kerberos mediante el administrador

kinit [administrator@LAB04.LAN](#)

```
Last login: Fri Feb 13 08:36:53 2026 from 18.206.107.28
ubuntu@ls04:~$ kinit administrator@LAB04.LAN
Password for administrator@LAB04.LAN:
Warning: Your password will expire in 41 days on Fri Mar 27 08:48:19 2026
ubuntu@ls04:~$
```

klist

```
ubuntu@ls04:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@LAB04.LAN

Valid starting     Expires            Service principal
02/13/26 09:10:06  02/13/26 19:10:06  krbtgt/LAB04.LAN@LAB04.LAN
                  renew until 02/14/26 09:10:01
ubuntu@ls04:~$
```