# Implementación de Servidor LDAP con Samba y Cliente

Este documento técnico detalla el proceso realizado para la configuración de un sistema de autenticación centralizado.
El proyecto abarca la implementación de un servidor LDAP (Lightweight Directory Access Protocol) integrado con Samba en un sistema Ubuntu, así como la posterior configuración de una máquina cliente para autenticarse contra dicho servidor.

## Parte 1: Configuración del Servidor LDAP con Samba

## 1. Preparación y Actualización del Sistema

El primer paso consistió en asegurar que el sistema operativo del servidor (Ubuntu) estuviera completamente actualizado para garantizar la estabilidad y seguridad. Se ejecutaron los siguientes comandos:

```
sudo apt update
sudo apt upgrade -y
sudo reboot
```

La opción -y se utilizó para automatizar la confirmación de las actualizaciones.

## 2. Instalación de Paquetes Esenciales

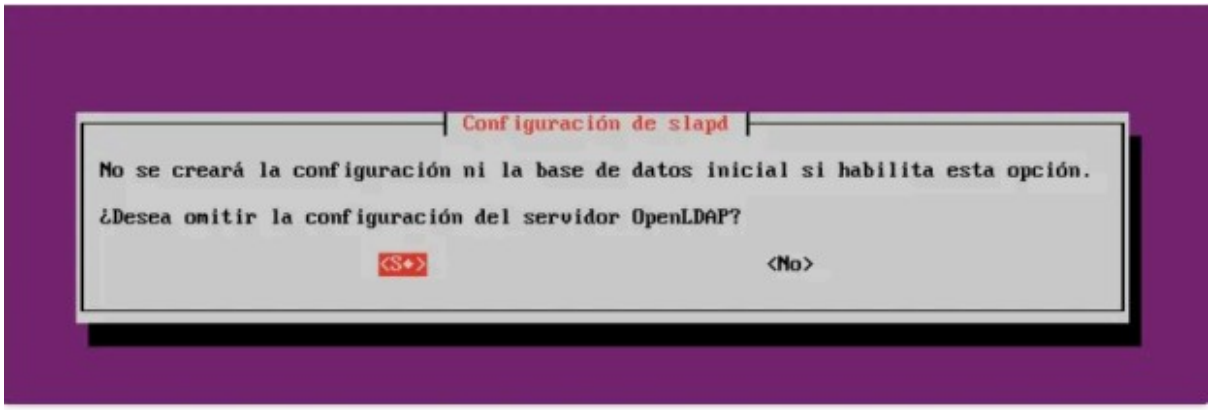
A continuación, se instalaron todos los paquetes necesarios para el funcionamiento de LDAP y su integración con Samba. Esto incluye el servidor LDAP ( slapd ), utilidades de gestión, y los componentes de Samba y Winbind

```
sudo apt install -y slapd ldap-utils samba smbclient
winbind libnsswinbind libpam-winbind
```

Durante la instalación, el sistema solicitó la creación de una contraseña de administrador para la base de datos LDAP, la cual es fundamental para su posterior gestión.

## 3. Instalación de Paquetes Esenciales

Para alinear el servicio LDAP con la estructura de la organización ficticia Luthor.corp, se procedió a reconfigurar slapd . Se optó por no utilizar la configuración por defecto para poder definir todos los parámetros desde cero.




### Justificación de la Elección del Motor de Base de Datos (HDB)

Durante la configuración, se eligió el motor de base de datos HDB. Aunque MDB es más moderno, se optó por HDB por las siguientes razones:

- **Madurez y Estabilidad**: Es el backend más probado y estable de OpenLDAP.
- **Funcionalidad Completa:** Soporta todas las características necesarias para una integración robusta con Samba.
- **Recuperación Robusta:** Ofrece un manejo superior ante fallos del sistema.
- **Soporte Comunitario:** Existe una amplia documentación y soporte por parte de la comunidad, facilitando la resolución de problemas.
- **Uso Empresarial:** Históricamente ha sido el motor recomendado para entornos de producción.

## 4. Configuración de Samba como Controlador de Dominio

Se modificó el archivo de configuración de Samba ( /etc/samba/smb.conf ) para que actuara como un controlador de dominio (DC) que utiliza LDAP como backend de autenticación. Se definieron el grupo de trabajo, el dominio (realm) y las directivas de mapeo de identificadores (idmap) para conectar Samba con los usuarios y grupos de LDAP.

```
[global]
        workgroup = luthor
        realm = luthor.corp
        netbios name = Ldap_Server
        security = user
        passdb backend = tdbsam
        domain master = yes
        domain logons = yes
        idmap config * : backend = tdb
        idmap config * : range = 1000-9999
        idmap config luthor : backend = ldap
        idmap config luthor : range = 10000-99999
        idmap config luthor : ldap_url = ldap://localhost
        idmap config luthor : ldap_base_dn = dc=luthor,dc=corp
        idmap config luthor : ldap_user_dn = cn=admin,dc=luthor,dc=corp
        ldap passwd sync = yes
        winbind enum users = yes
        winbind enum groups = yes
        winbind use default domain = yes
        add machine script = /usr/sbin/useradd -c "Machine" -d/var/lib/samba - s
        /bin/false %u

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

[netlogon]
        path = /var/lib/samba/netlogon
        read only = no

[homes]
        comment = Home Directories
        browseable = no
        writable = yes
```

## 5. Diagnóstico y Solución de Error de Esquema

### Error Detectado: Esquema de Samba Ausente

Al intentar cargar la estructura inicial de Samba a LDAP, el servidor devolvió un error de "Sintaxis Inválida".

**Causa identificada**:

*ldapsearch -Q -LL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config*

Mediante el comando de ldapsearch se evidencio que faltaban los schemas de samba ya que únicamente mostraba los esquemas básicos.

Los esquemas de Samba se localizaron en */usr/share/doc/samba/examples/LDAP* ,y estaban comprimidos ( .gz ).

### Solucion Aplicada

El problema se resolvió siguiendo estos pasos:

1. Descomprimir los archivos samba.ldif.gz y samba.schema.gz .

*sudo gzip -d samba.ldif.gz*
*sudo gzip -d samba.schema.gz*

2. Copiar los archivos resultantes ( samba.ldif y samba.schema ) al directorio de esquemas de LDAP ( /etc/ldap/schema/ ).

*cp -d samba.ldif /etc/ldap/schema/*
*cp -d samba.schema /etc/ldap/schema/*

3. Agregar el esquema a la configuración de LDAP

*sudo ldapadd -Y EXTERNAL -H ldapi:/// -f etc/ldap/schema/samba.ldif*

Tras aplicar el esquema, el comando para agregar las unidades organizativas y grupos de Samba se ejecutó exitosamente.

## 6. Configuración de Samba como Controlador de Dominio

Con el esquema corregido, se crearon las Unidades Organizativas (OUs) para usuarios y grupos. Posteriormente, se sincronizó la contraseña de administrador de LDAP con Samba usando *sudo smbpasswd -w {contraseña} .* Finalmente, se verificó que los usuarios creados en LDAP fueran visibles tanto para el sistema Linux como para Samba.

### Verificación en Linux:

*getent passwd*

```
administrador-ldap:x:1000:1000:administrador-ldap,,,:/home/administrador-ldap:/bin/bash
openldap:x:112:119:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
Useradministracion0 :x:3000:2000:N0 A0:/home/user0:/bin/bash
Useradministracion1 :x:3001:2000:N1 A1:/home/user1:/bin/bash
Useradministracion2 :x:3002:2000:N2 A2:/home/user2:/bin/bash
Userdesarrollo0 :x:3009:2003:N0 A0:/home/user0:/bin/bash
Userdesarrollo1 :x:3010:2003:N1 A1:/home/user1:/bin/bash
Userdesarrollo2 :x:3011:2003:N2 A2:/home/user2:/bin/bash
Userdesarrollo3 :x:3012:2003:N3 A3:/home/user3:/bin/bash
Userdesarrollo4 :x:3013:2003:N4 A4:/home/user4:/bin/bash
Userrecursos-humanos0 :x:3007:2002:N0 A0:/home/user0:/bin/bash
Userrecursos-humanos1 :x:3008:2002:N1 A1:/home/user1:/bin/bash
Usersoporte0 :x:3003:2001:N0 A0:/home/user0:/bin/bash
Usersoporte1 :x:3004:2001:N1 A1:/home/user1:/bin/bash
Usersoporte2 :x:3005:2001:N2 A2:/home/user2:/bin/bash
Usersoporte3 :x:3006:2001:N3 A3:/home/user3:/bin/bash
administrador-ldap@ServidorLdap:~$ _
```

### Verificación en Samba:

```
administrador-ldap@ServidorLdap:~$ sudo pdbedit  -L
Useradministracion0 :3000:N0 A0
Useradministracion1 :3001:N1 A1
Useradministracion2 :3002:N2 A2
Userdesarrollo0 :3009:N0 A0
Userdesarrollo1 :3010:N1 A1
Userdesarrollo2 :3011:N2 A2
Userdesarrollo3 :3012:N3 A3
Userdesarrollo4 :3013:N4 A4
Userrecursos-humanos0 :3007:N0 A0
Userrecursos-humanos1 :3008:N1 A1
Usersoporte0 :3003:N0 A0
Usersoporte1 :3004:N1 A1
Usersoporte2 :3005:N2 A2
Usersoporte3 :3006:N3 A3
administrador-ldap@ServidorLdap:~$
```

# Parte 2: Configuración del  Cliente LDAP

## 1.Preparación del Cliente y Configuración de Red

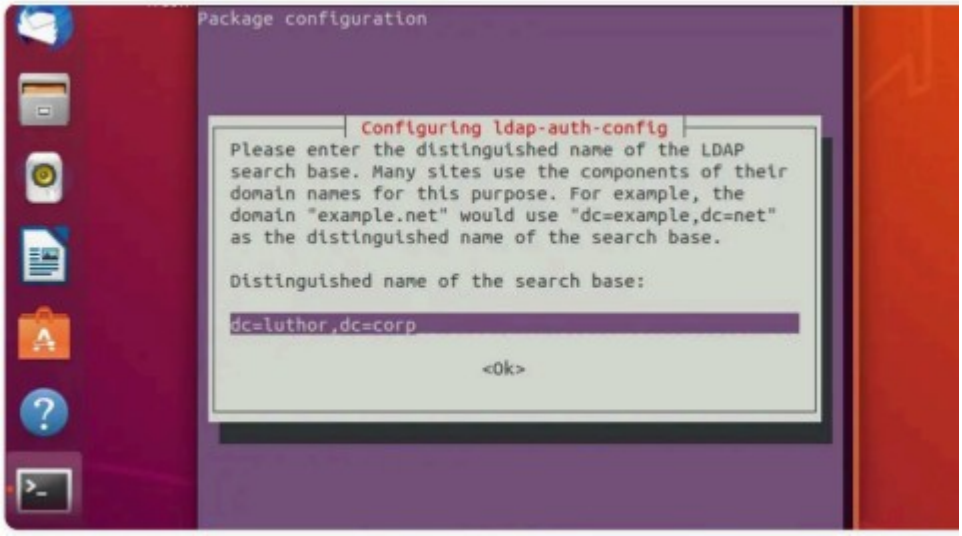
Se instaló un sistema operativo cliente y se creó un usuario administrador local. Un paso crucial fue modificar la configuración de red de la máquina virtual de NAT a Adaptador Puente para que el cliente y el servidor pudieran comunicarse en la misma red con IPs únicas.


## 2. Instalación de Dependencias y Configuración

Se actualizaron los repositorios y se instalaron las librerías necesarias para la autenticación LDAP:

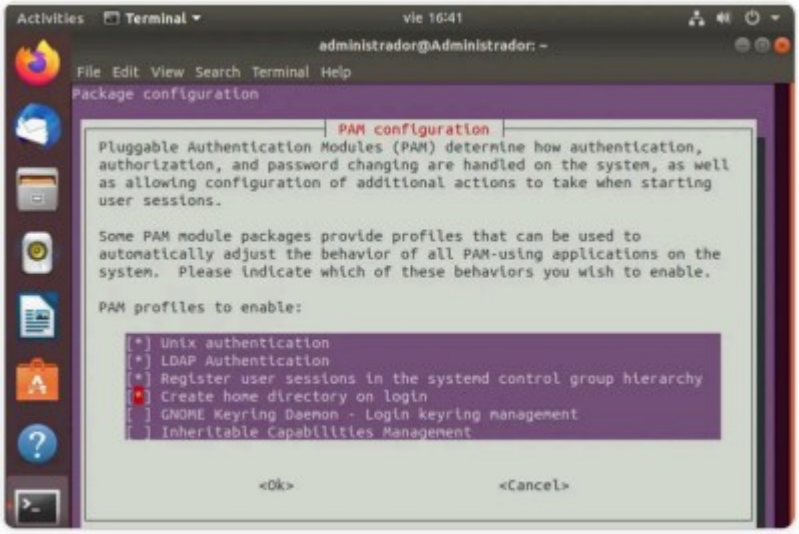
*sudo apt update*
*sudo apt install libnss-ldap libpam-ldap ldap-utils*

Durante la instalación, un asistente guió la configuración, solicitando la URI del servidor LDAP *( ldap://IP_DEL_SERVIDOR/ )* y el DN base *( dc=luthor,dc=corp )*.

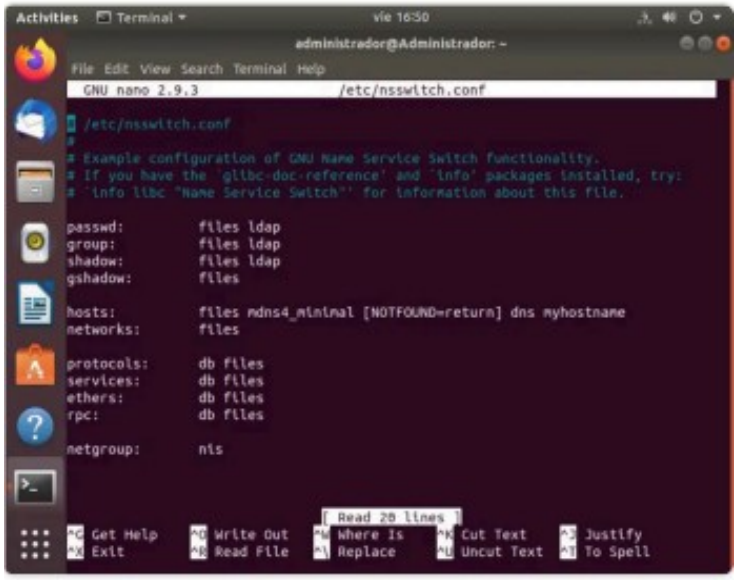



## 3. Configuración de PAM y NSS

Se utilizó sudo pam-auth-update para configurar los módulos de autenticación. Se habilitó la opción "Create home directory on login" para que los usuarios de LDAP tuvieran un directorio personal al iniciar sesión por primera vez.



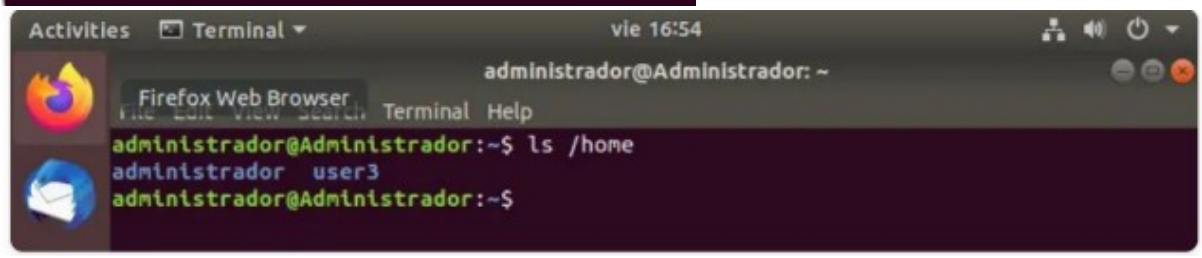

Adicionalmente, se modificó el archivo /etc/nsswitch.conf para indicar al sistema que buscara información de usuarios, grupos y contraseñas primero en los archivos locales y luego en LDAP ( files ldap ).




## 4. Verificación de Usuarios y Acceso

Se instaló el servicio nslcd ( *sudo apt install nslcd* ) para mejorar la integración con la interfaz de inicio de sesión. Una verificación con getent passwd confirmó que los usuarios del servidor LDAP eran visibles en el cliente.

El inicio de sesión con un usuario de LDAP *(Usersoporte3)* fue exitoso, y se confirmó la creación automática de su directorio personal en /home

# Parte 2: Montar Recurso Compartido

## 1.Montaje de Recurso Compartido

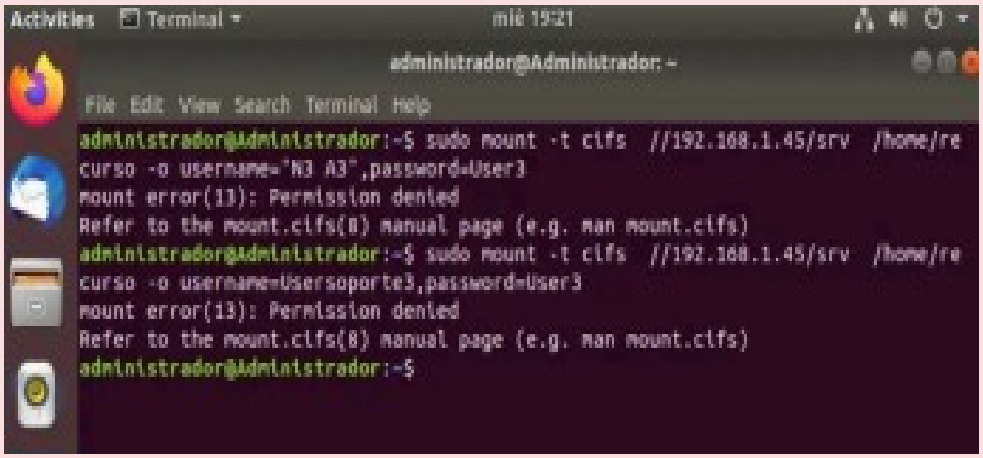
Para montar una carpeta compartida desde el servidor Samba en la máquina cliente se debe  instalar el paquete cifs-utils , que proporciona las herramientas necesarias para montar sistemas de archivos usando CIFS

*sudo apt install cifs-utils*

## 2. Diagnóstico y Solución de Error Permiso al montar

### Error Detectado: Montado falla por permiso denegado

Al intentar montar el recurso  aun con credenciales validas no me daba permiso.



El problema se origino por una inconsistencia entre las credenciales de LDAP y las credenciales almacenadas en Samba, lo que causaba fallos de autenticación y errores al montar el recurso compartido.
Además, la carpeta compartida presentaba permisos incorrectos.

## Solucion:

**1.** Se resincronizó el usuario en Samba, recreando su entrada y habilitándola nuevamente:

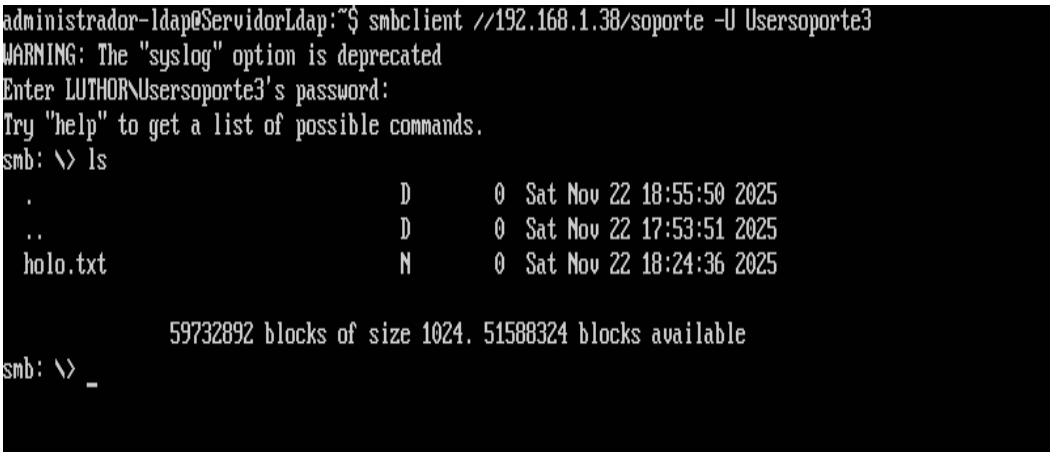
*sudo smbpasswd -a usuario*
*sudo smbpasswd -e usuario*

**2.** Se eliminó y recreó la carpeta compartida en el servidor, asegurando permisos
correctos y agregando un archivo como prueba

*sudo mkdir soporte*
*sudo touch /srv/soporte/holo.txt*
*sudo chown root : soporte /srv/soporte*
*sudo chmod 2770 /srv/soporte*

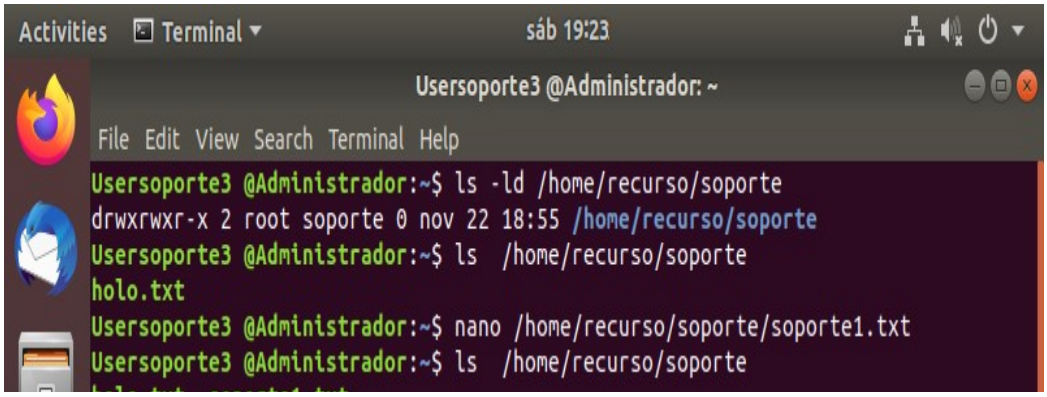
**3.** Se reconfiguro el smb.conf del recurso

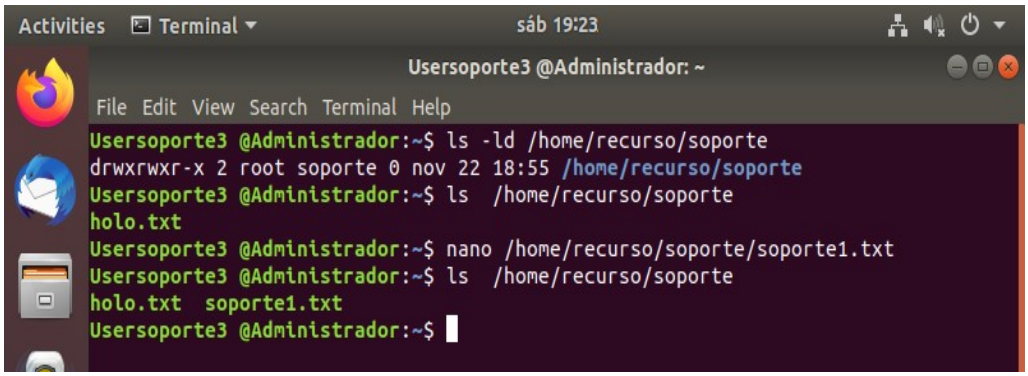
*[soporte]*
*path = /ruta/completa/soporte*
*browseable = yes*
*read only = no*
*valid users = @soporte*
*force group = soporte*
*create mask = 0660*
*directory mask = 0770*




**4.** Se volvió a montar el recurso en el cliente, verificando que los archivos creados en el punto de montaje se reflejaran correctamente en el servidor.

*sudo mount -t cifs //server/soporte /home/recurso/soporte -o username=usuario,password=XXXX,gid=idgrupoLDAP ,file_mode=0770,dir_mode=2770*




```
administrador-ldap@ServidorLdap:~$ smbclient //192.168.1.38/soporte -U Usersoporte3
WARNING: The "syslog" option is deprecated
Enter LUTHOR\Usersoporte3's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Nov 22 18:55:50 2025
  ..                                  D        0  Sat Nov 22 17:53:51 2025
  holo.txt                            N        0  Sat Nov 22 18:24:36 2025

                59732892 blocks of size 1024. 51588324 blocks available
smb: \> ls
  .                                   D        0  Sat Nov 22 19:23:03 2025
  ..                                  D        0  Sat Nov 22 17:53:51 2025
  holo.txt                            N        0  Sat Nov 22 18:24:36 2025
  soporte1.txt                        N       12  Sat Nov 22 19:22:59 2025

                59732892 blocks of size 1024. 51588304 blocks available
smb: \>
```