

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

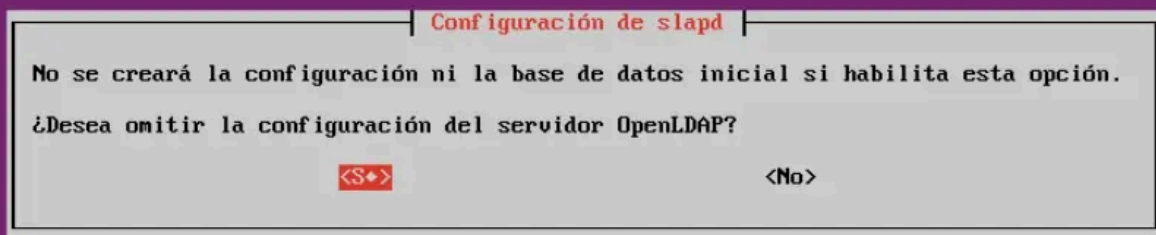
A continuación, se instalaron todos los paquetes necesarios para el funcionamiento de LDAP y su integración con Samba. Esto incluye el servidor LDAP (`slapd`), utilidades de gestión, y los componentes de Samba y Winbind.

```
sudo apt install -y slapd ldap-utils samba smbclient winbind libnss-
winbind 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. Reconfiguración de LDAP

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

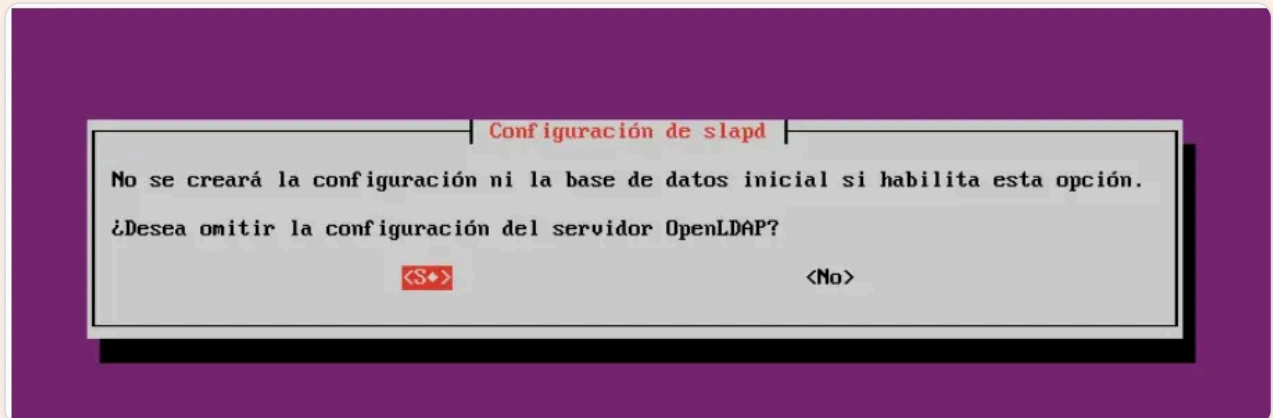
[homes]
    comment = Home Directories
    browseable = no
    writable = yes
```

5. Diagnóstico y Solución de Error de Esquema

Error Detectado: Esquema de Samba Ausente

Al intentar agregar la estructura inicial de Samba a LDAP, se encontró un error de "Sintaxis Inválida". Una investigación reveló que el esquema de Samba no estaba cargado en la configuración de LDAP. La verificación se realizó con el comando `ldapsearch`, que mostró únicamente los esquemas básicos.

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

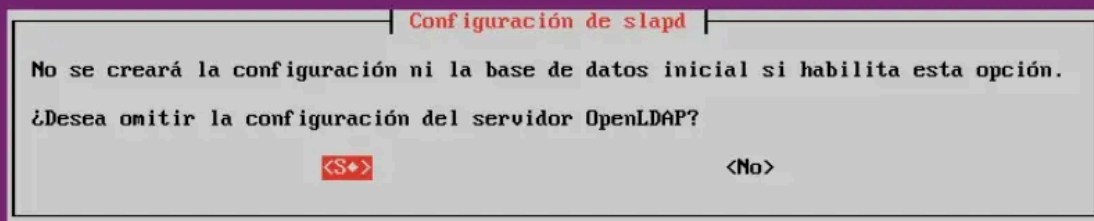


Solución Aplicada

El problema se resolvió siguiendo estos pasos:

1. Descomprimir los archivos `samba.ldif.gz` y `samba.schema.gz`.
2. Copiar los archivos resultantes (`samba.ldif` y `samba.schema`) al directorio de esquemas de LDAP (`/etc/ldap/schema/`).
3. Agregar el esquema a la configuración de LDAP utilizando el comando `ldapadd`.

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

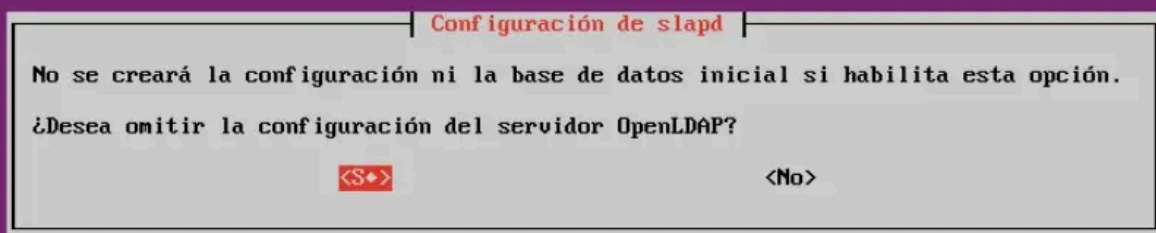


6. Creación de Estructura LDAP y Verificación Final

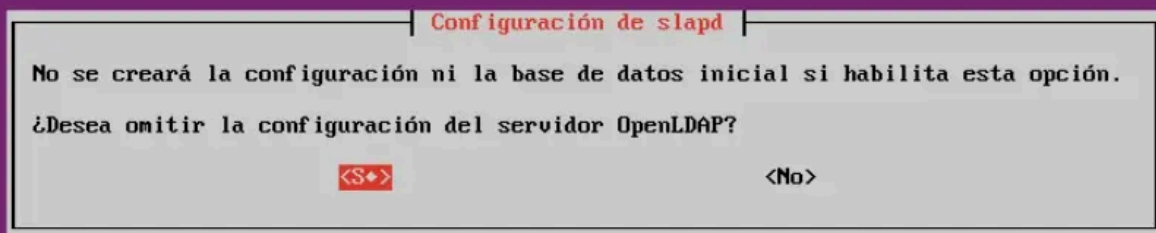
Con el esquema corregido, se crearon las Unidades Organizativas (OUs) para usuarios y grupos. Posteriormente, se sincronizó la contraseña de administrador de LDAP con Samba usando `sudo smbpasswd -w {contraseña}`.

Finalmente, se verificó que los usuarios creados en LDAP fueran visibles tanto para el sistema Linux como para Samba.

Verificación en Linux:



Verificación en Samba:



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.



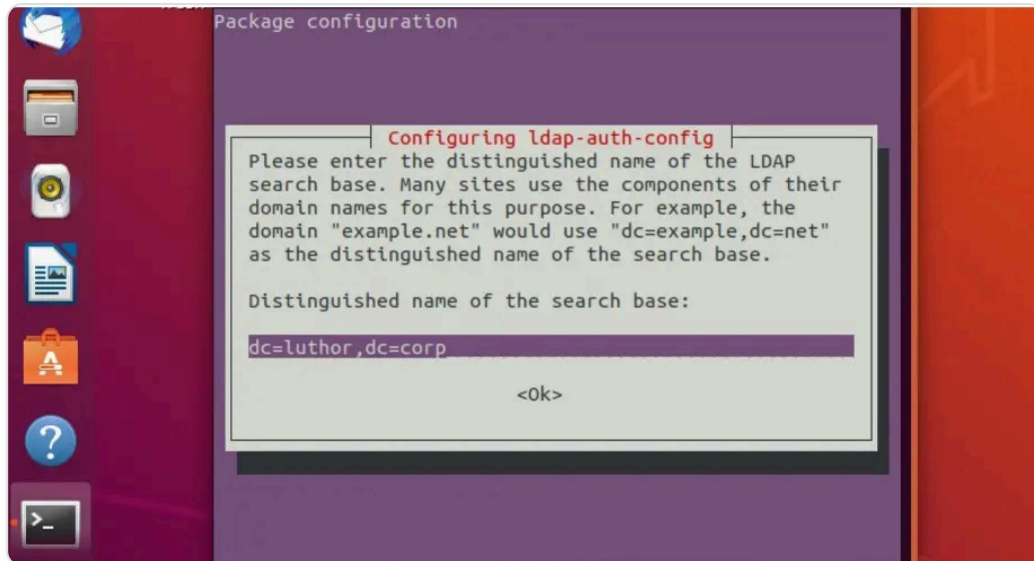
2. Instalación de Dependencias y Configuración

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

```
sudo apt update
```

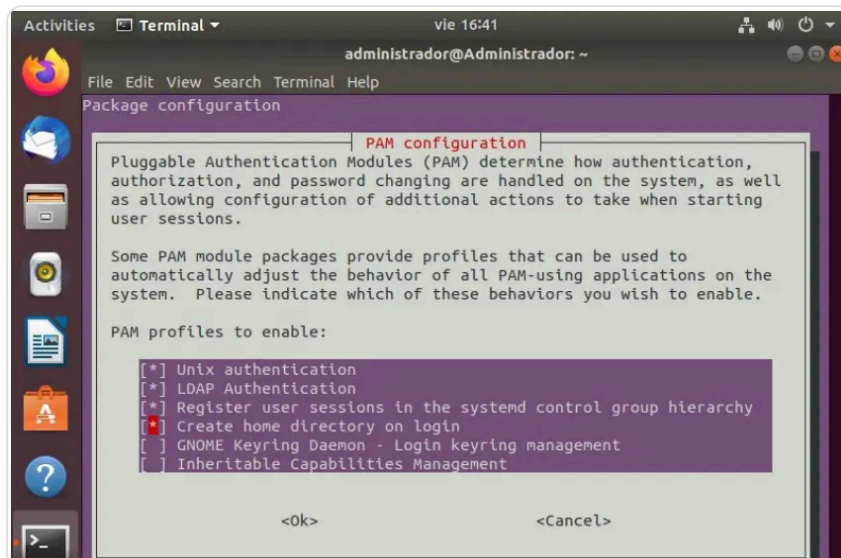
```
sudo apt install libnss-ldap libpam-ldap ldap-utils
```

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`).

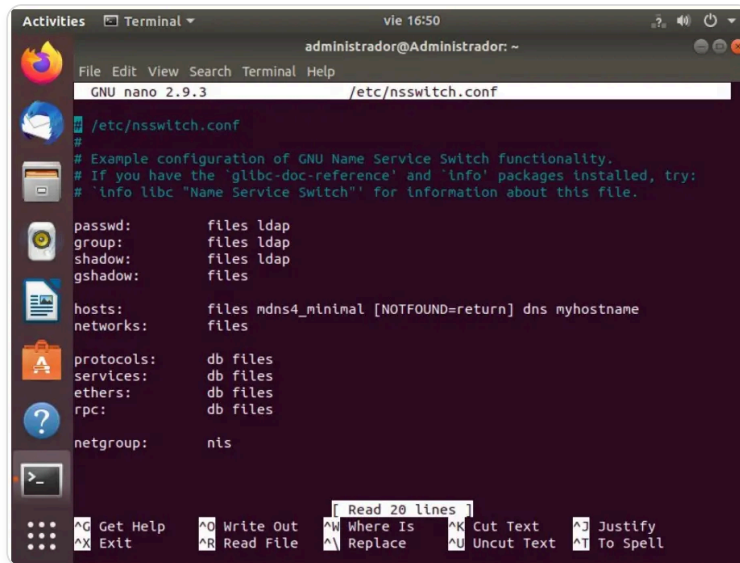


3. Configuración de PAM y NSS

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`).



```
Activities Terminal vie 16:50
administrador@Administrador: ~
GNU nano 2.9.3 /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 ldap
group:       files ldap
shadow:      files ldap
gshadow:     files

hosts:       files mdns4_minimal [NOTFOUND=return] dns myhostname
networks:    files

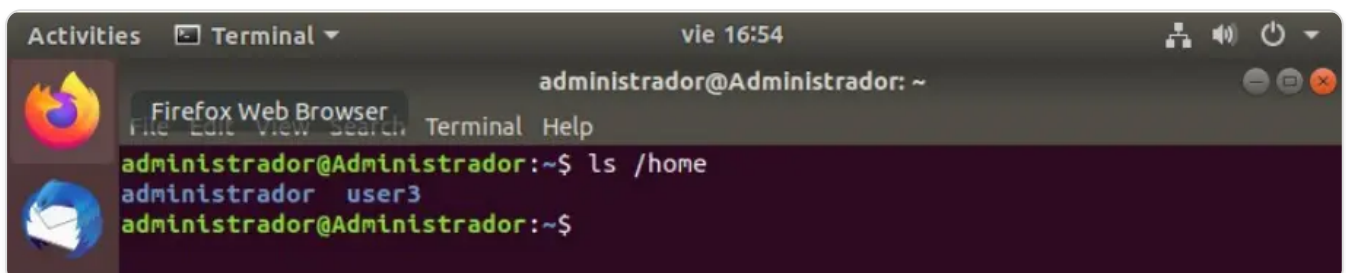
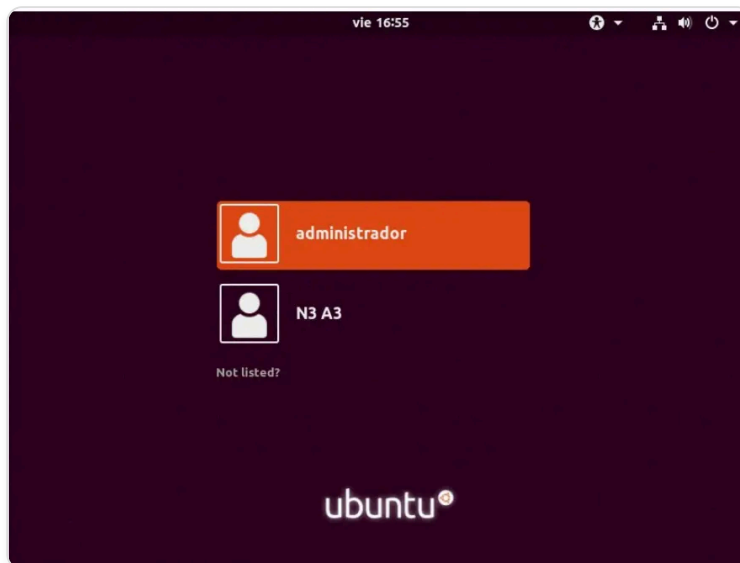
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

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`.



```
Activities Terminal vie 16:54
administrador@Administrador: ~
Firefox Web Browser
administrador@Administrador:~$ ls /home
administrador  user3
administrador@Administrador:~$
```


Parte 3: Incidencia Final y Conclusión del Proyecto

1. Intento de Montaje de Recurso Compartido

El paso final del proyecto consistía en montar una carpeta compartida desde el servidor Samba en la máquina cliente. Para ello, se instaló el paquete `cifs-utils`, que proporciona las herramientas necesarias para montar sistemas de archivos CIFS.

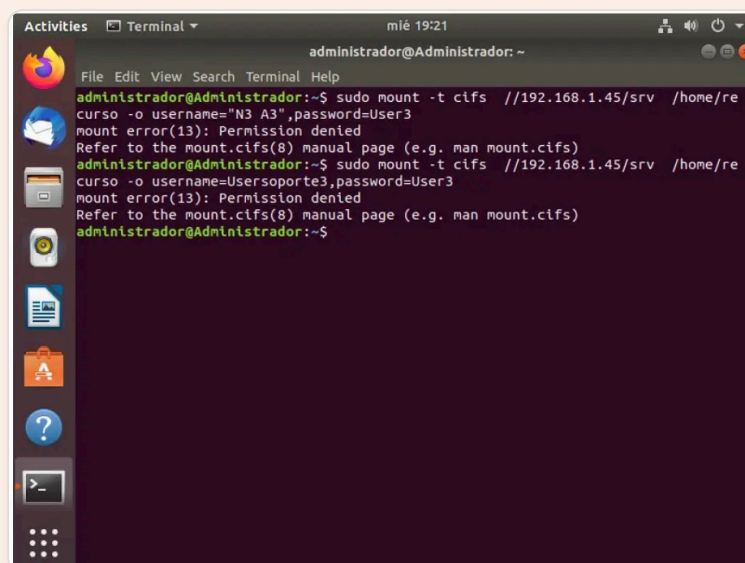
```
sudo apt install cifs-utils
```

Se intentó montar el recurso compartido utilizando el comando `mount` con las credenciales de un usuario de LDAP válido.

2. Error No Resuelto y Cierre del Proyecto

Incidencia: `mount error(13): Permission denied`

A pesar de utilizar credenciales correctas y probar con diferentes usuarios, el intento de montaje fracasó consistentemente, devolviendo el error **"Permission denied" (Permiso denegado)**.



```
administrador@Administrador: ~  
File Edit View Search Terminal Help  
administrador@Administrador:~$ sudo mount -t cifs //192.168.1.45/srv /home/recurso -o username="N3 A3",password=User3  
mount error(13): Permission denied  
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)  
administrador@Administrador:~$ sudo mount -t cifs //192.168.1.45/srv /home/recurso -o username=Usersoporte3,password=User3  
mount error(13): Permission denied  
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)  
administrador@Administrador:~$
```

Se llevó a cabo una investigación exhaustiva para identificar la causa de este error, revisando permisos en el servidor, configuraciones de Samba y posibles problemas de

autenticación a nivel de CIFS. Sin embargo, no se logró encontrar una solución documentada que resolviera el problema en el contexto de esta configuración específica.

Conclusión: Dado que la funcionalidad principal de autenticación centralizada de usuarios a través de LDAP y Samba se implementó con éxito, y ante la incapacidad de superar el obstáculo del montaje de recursos compartidos tras agotar las vías de investigación disponibles, se ha tomado la decisión de concluir el proyecto en esta fase. La incidencia queda documentada como un punto pendiente que requeriría un análisis más profundo fuera del alcance de esta implementación.