

# Actividad - LDAP. Conectar cliente Ubuntu a Openldap server:

## 1. Introducción:

Esta guía detalla el procedimiento técnico para configurar la estación de trabajo Ubuntu (cliente) con IP 192.168.10.64 para autenticar usuarios centralizados alojados en el servidor OpenLDAP (192.168.10.59)

Esta guía asume que el servidor OpenLDAP está operativo y configurado con el dominio base: **dc=asix,dc=local**

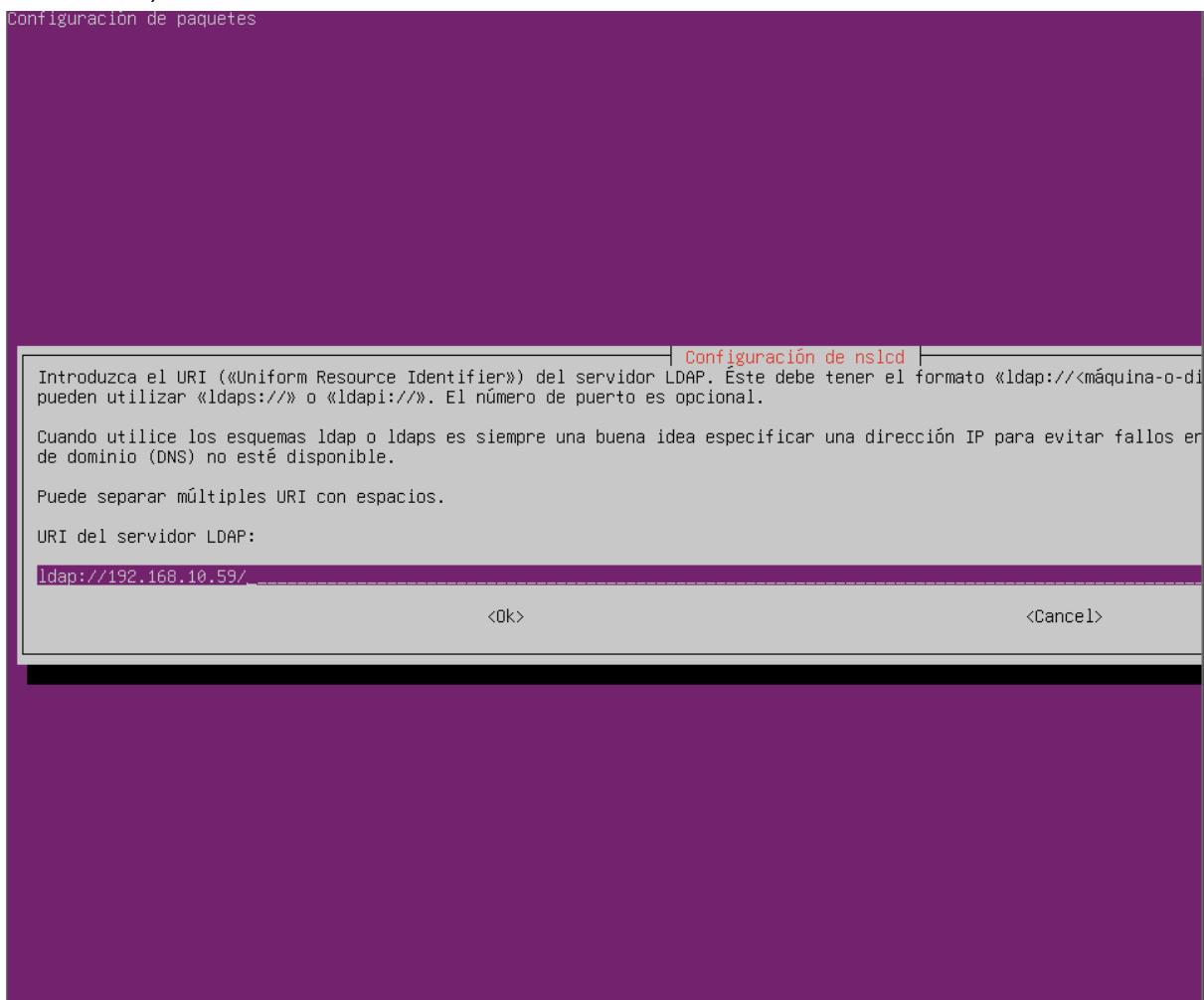
## 2. Configuración:

1. En el cliente ejecutamos el comando “`sudo nano /etc/hosts`” y añadimos lo siguiente al final del archivo: “192.168.10.59 ldap-server.asix.local ldap-server”

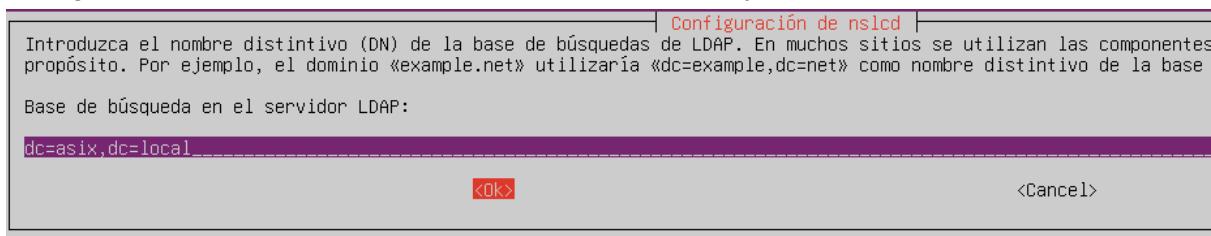
```
GNU nano 7.2                               /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntulab
192.168.10.59 ldap-server.asix.local ldap-server_
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

2. Instalamos las librerías LDAP con el siguiente comando: “`sudo apt update`” para actualizar la lista de repositorios y ejecutamos “`sudo apt install libnss-ldapd libpam-ldapd nscd`” para ejecutar la instalación:

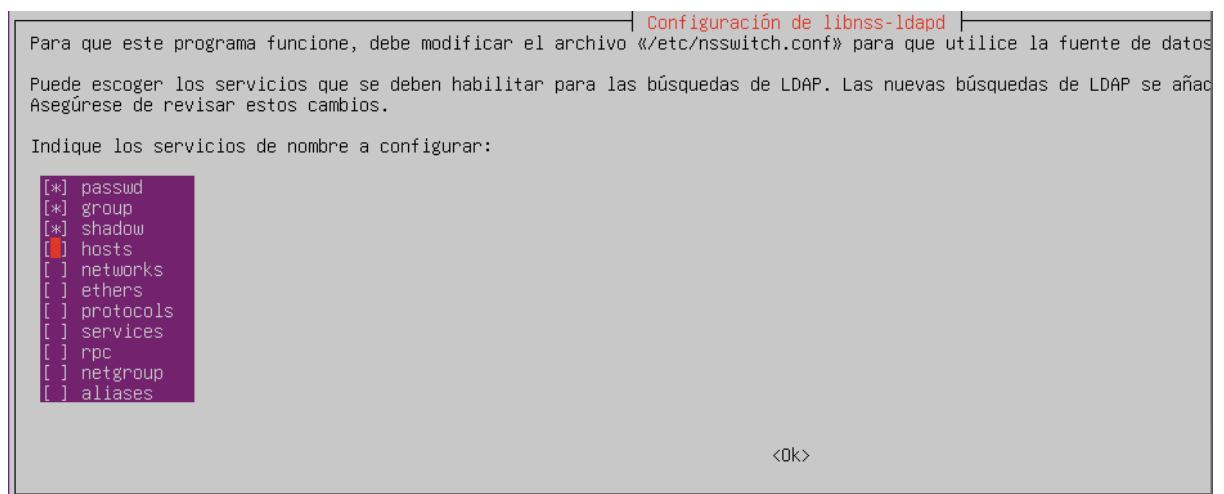
3. Nos pedirá la URL del servidor LDAP, la introducimos en este formato:  
“**ldap://192.168.10.59/**” (podríamos poner tambien  
“**ldap://ldap-server.asix.local/**” pero ponemos la IP directa para evitar problemas con el DNS):



4. Configuramos la base de búsqueda: “**dc=asix,dc=local**” y pulsamos ok:



5. Marcamos “**passwd**”, “**group**” y “**shadow**” pulsando con barra espaciadora sobre ellos:



Configuración de libnss-ldapd

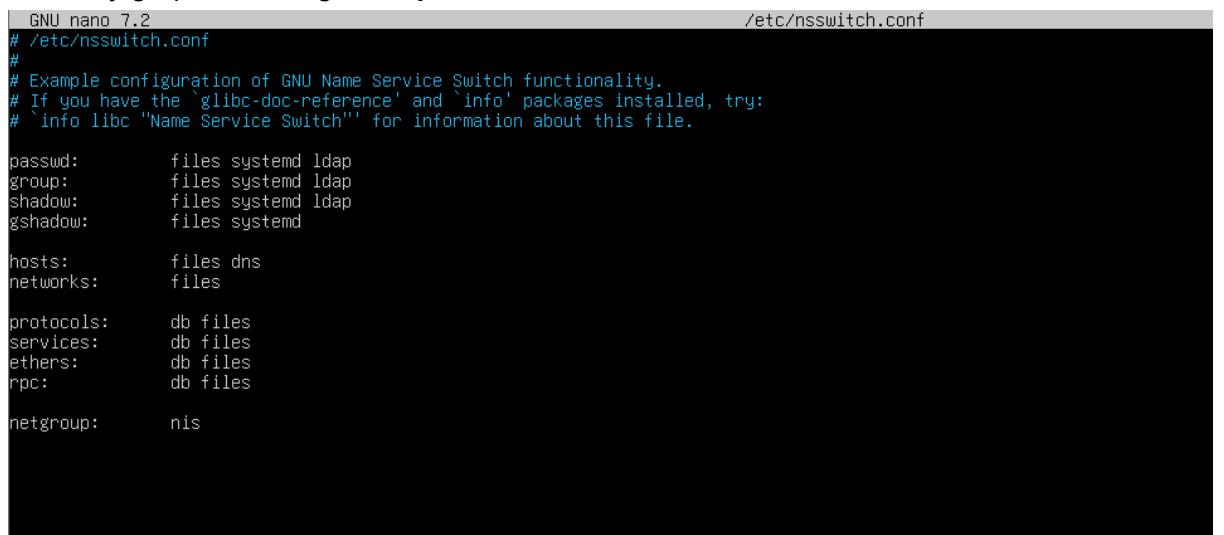
Para que este programa funcione, debe modificar el archivo «/etc/nsswitch.conf» para que utilice la fuente de datos Asegúrese de revisar estos cambios.

Indique los servicios de nombre a configurar:

```
[*] passwd
[*] group
[*] shadow
[ ] hosts
[ ] networks
[ ] ethers
[ ] protocols
[ ] services
[ ] rpc
[ ] netgroup
[ ] aliases
```

<Ok>

6. Ejecutamos “**sudo nano /etc/nsswitch.conf**” y comprobamos que las líneas de usuario y grupos contengan **ldap**:



```
GNU nano 7.2
# /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  ldap
group:       files  systemd  ldap
shadow:      files  systemd  ldap
gshadow:     files  systemd

hosts:        files  dns
networks:    files

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

netgroup:    nis
```

- Como los usuarios del dominio LDAP no tienen una carpeta personal creada físicamente en el cliente, se debe configurar PAM para generarla automáticamente en el primer inicio de sesión, para ello ejecutamos “**sudo nano /etc/pam.d/common-session**” y añadimos la siguiente linea alfinal del documento:  
**“session optional pam\_mkhomedir.so skel=/etc/skel umask=077”:**

```
GNU nano 7.2                                         /etc/pam.d/common-session *
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of interactive sessions.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1]          pam_permit.so
# here's the fallback if no module succeeds
session requisite             pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required              pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional              pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required              pam_unix.so
session [success=ok default=ignore]    pam_ldap.so minimum_uid=1000
session optional              pam_systemd.so
session optional              pam_mkhomedir.so skel=/etc/skel umask=077_
# end of pam-auth-update config
```

- Aplicamos estos cambios reiniciando LDAP: “**sudo systemctl restart nscd**” y “**sudo systemctl restart nsldc**”:

```
rafi@ubuntulab:~$ sudo systemctl restart nscd
rafi@ubuntulab:~$ sudo systemctl restart nsldc
rafi@ubuntulab:~$ _
```

- Comprobamos la conexión entre cliente (.64) y servidor (.59), para ello usaremos el comando “**getent passwd jdoe**”. Si esta bien configurado, nos devolverá la información del usuario del servidor:

```
rafi@ubuntulab:~$ getent passwd jdoe
jdoe:x:10000:5000:John Doe:/home/jdoe:/bin/bash
```

- Ahora suplantamos la identidad del usuario **jdoe** para verificar el acceso y la creación del directorio home usando el comando: “**su - jdoe**”:

```
rafi@ubuntulab:~$ su - jdoe
Password:
Creating directory '/home/jdoe'.
jdoe@ubuntulab:~$ _
```

Para acabar de comprobar que está bien configurado, abriremos una terminal de windows shell y nos conectaremos al cliente usando el usuario de LDAP: “**ssh jdoe@192.168.10.64**”. Nos pedirá la contraseña del usuario y si queremos guardar la fingerprint, decimos “**Yes**” y ya estaremos conectados a la máquina a través de SSH, mediante el usuario de LDAP:

```
PS C:\Users\rafik> ssh jdoe@192.168.10.64
The authenticity of host '192.168.10.64 (192.168.10.64)' can't be established.
ED25519 key fingerprint is SHA256:xfMvk4f1SPGCKEWBWligiu0+wThfbdE1mpdOF9nR8/E.
This host key is known by the following other names/addresses:
  C:\Users\rafik/.ssh/known_hosts:4: 192.168.1.40
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.10.64' (ED25519) to the list of known hosts.
jdoe@192.168.10.64's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of lun 01 dic 2025 18:50:12 UTC

System load:  0.08          Processes:           123
Usage of /:   44.2% of 11.21GB  Users logged in:      1
Memory usage: 12%          IPv4 address for enp0s3: 192.168.10.64
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge
```

```
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

6 actualizaciones de seguridad adicionales se pueden aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm
```

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/\*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

```
jdoe@ubuntulab:~$ 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 08:00:27:07:b3:2d brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.64/24 metric 100 brd 192.168.10.255 scope global dynamic enp0s3
        valid_lft 18786sec preferred_lft 18786sec
        inet6 fe80::a00:27ff:fe07:b32d/64 scope link
            valid_lft forever preferred_lft forever
jdoe@ubuntulab:~$
```

Esto nos hará más fácil administrar y monitorizar los usuarios de diferentes VM.